AccessZone® – PcManagement™ User Manual

User Manual for AccessZone® PcManagement™ PC tool version 3.0.48 and above

2015-07-02 US 0.23

 MVC-Data ApS Skalhuse 5 9240 Nibe Denmark Web www.mvc-data.com E-mail info@mvc-data.com Phone +45 25 12 84 02

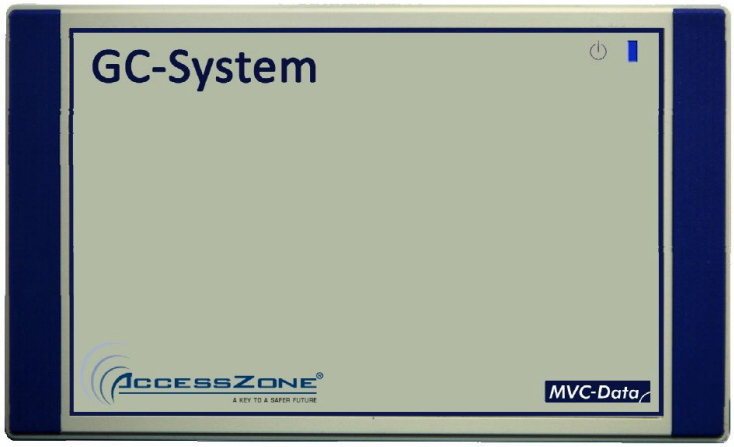
AccessZone® System - *A Key to a Safer Future*

Congratulations on choosing an AccessZone® Access Control System. It is a flexible and easy to use system for controlling access to doors and gates to private homes, shops and companies or handling different alarm in CarsZone™ or SafeZone™ systems.

Look forward to the quick setup using the intuitive and graphical user interface and the system's many built features.

This is the user manual for how to use and configure the AccessZone® PC software application PcManagement™. It covers all AccessZone® access control systems with a PC interface RS232/RS422/LAN/Wi-Fi and Bluetooth in the GateController™ series:

GC630/GC640/GC670/GC680/GC690



GC3000

AccessZone GateController box located near door or gate

Please see the PcManagement™ PC Installation Manual for instructions on how to install the software on a Windows XP SP2, Vista, 7, 8 or Windows Server 2012 PC.

Get easy and seamless accesses to the secured area with your mobile phone working as a secure access key from a distance from 0.1 up to 10 meters

Table of Contents

1 Disclaimers

MVC-Data ApS assumes no responsibility for any errors in this manual.

MVC-Data ApS is constantly working to improve its products and offer new features in collaboration with customers and partners. Therefore, MVC-Data ApS reserves the right to change the hardware, software and / or specifications without notice and shall have no obligation to update the information contained in this manual.

MVC-Data ApS's products are not authorized for use as system-critical components in life supporting devices or systems.

AccessZone® is a registered trademark of MVC-Data ApS. PcManagement™, CareZone™ and SafeZone™ are trademarks of MVC-Data ApS.

The Bluetooth trademark is owned by the Bluetooth SIG. All other trademarks are owned by their respective owners.

The displayed screen images may differ.

2 Introduction

The AccessZone® Access Control Systems are well suited for use in private homes, shops and companies and can be scaled from a single GateController™ to multiple GateControllers.

They are unique wireless access control systems built on Bluetooth wireless technology – a wireless technology that operates in the license free ISM band at 2.4 GHz.

The systems only allow access to users who can be identified by their unique Key ID and optional a 4 digit PIN code for increased security. The used mobile phones or other Bluetooth devices must be set to “visible” to allow them to be discovered by the system.

This eliminates the need for mechanical readers and keyboards outside the secured area. This removes the risk for property damage and breakdown due to harsh environmental conditions and heavy use.

PcManagement is also used in CareZone™ or SafeZone™ systems handling real time alarms from users wearing a GC110 or GC120 tag in e.g. nursing homes or safeguarding machines.

A feature might require a firmware update of your system to be supported. Please refer to the GC630/GC640/GC660/GC670/GC690 or GC3000 firmware Release Note for the latest updates.

3 What is PcManagement™

AccessZone® PcManagement™ System is the PC application/server that handles the user interface for the AccessZone® GateController™ systems, which are connected to gates, barriers, locks and other locking mechanisms.

3.1 Properties:

- Easy and seamless access with your Bluetooth® enabled mobile phone, tablet or GPS – No tags or cards needed
- Fully featured access control system with booking feature
- Exceptional, fast and unique mobile identification with Bluetooth®
- Up to 16 character Admin PIN code for secure use or view only operator mode (default)
- High security with individual user access PIN code and tamper alarm
- Scalable for up to 2000 simultaneous users – all stored locally in the GateController
- Fast registration of a new key at the gate within a few seconds (open doors or alarms)
- Unique time profiles for each GateController™
- Individual and group user access profiles
- Grant and revoke user access at a glance
- Grant instant access from the graphical user interface
- Voluntary SMS or E-mail on selected events
- Control and monitor multiple gates from a single PC
- Register all events in database for later analysis
- Stores all access in a database for later analysis
- Supports typical database functions – search who and what gate etc.
- Provides simultaneous support for multiple GateControllers
- Advanced system settings are configurable via XML file
- Server option for remote control of access via LAN/WAN
- Supports PC interface with RS232/RS422/LAN/Wi-Fi (IP) or Bluetooth
- Robust housing (IP40 indoor use/IP65 outdoor use depending on system type)
- Easy firmware upgrade with bootloader
- Low installation and maintenance costs
- RoHS compliant and low power consumption

Please refer to the:

- AccessZone® PcManagement™ PC Installation Manual for instructions on how to install the application on a PC. Refer to AccessZone PcManagement PC Installation Manual

- AccessZone® - Remote™ client User Manual for instructions on how to use the remote client application. Refer to AccessZone - Remote User Manual

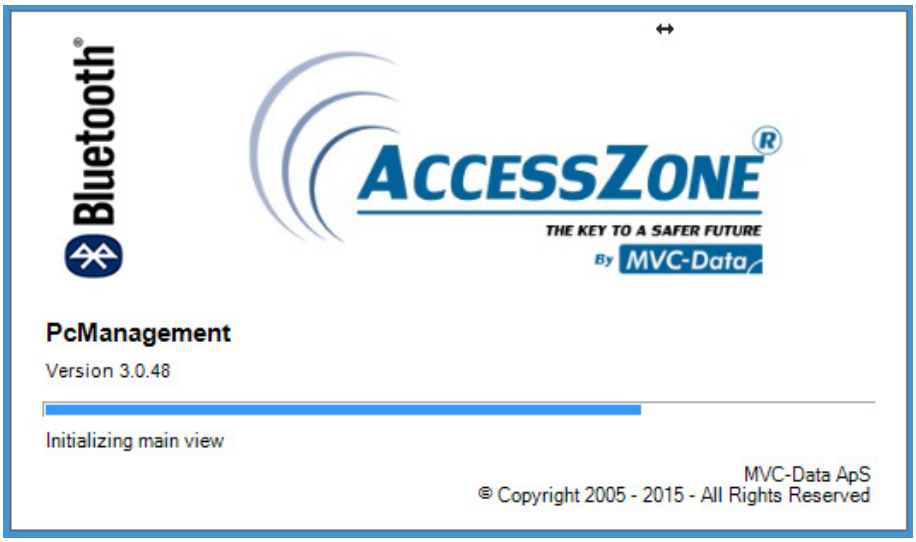
- GC630/GC640/GC660/GC670/GC680/GC690 or GC3000 Series Installation Manual for instructions on how to install the system:
    - AccessZone GC630/GC640/GC660/GC670/GC680/GC690 Installation Manual
    - AccessZone GC3000 Installation Manual

More information on: http://www.mvc-data.com/Manuals.html

4 PcManagement™

4.1 Start-Up

The program can be started by clicking the AccessZone® PC Management short cut on the desktop or from Windows All Program “MVC-Data AccessZone” application menu. It can also be started by double clicking on the file PcManagement.exe in the installation directory. Or it can be automaticall started with e.g. Windows Task Scheduler on power up:



The image above shows the AccessZone® PcManagement™ System start-up screen. The system is initialized according to information in the config.xml configuration file and opens the database with GateControllers and user information.

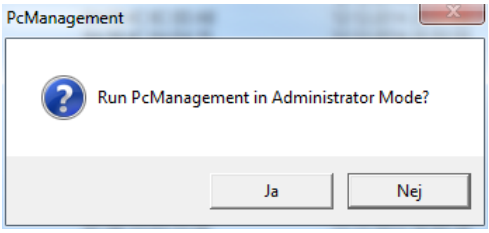
Some menus and functions must be enabled in the system configuration file config.xml. Typical path c:\ProgramData\AccessZone\config.xml.

Note!
Do not edit config.xml while PcManagement is running.

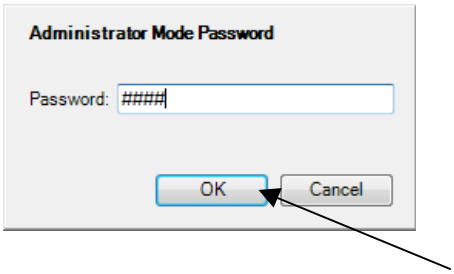
4.2 Operator Mode and Administrator Mode - How to Switch Mode

The default startup mode is Operator Mode where changes made to users and/or configuration is prohibited.

When startet - you can switch to Administrator Mode by clicking menu "Switch to Admin Mode..." from the "Settings" menu or by clicking Ctrl+M.



Click "Yes" to enter Administrator Mode or "No" to stay in Operator Mode.



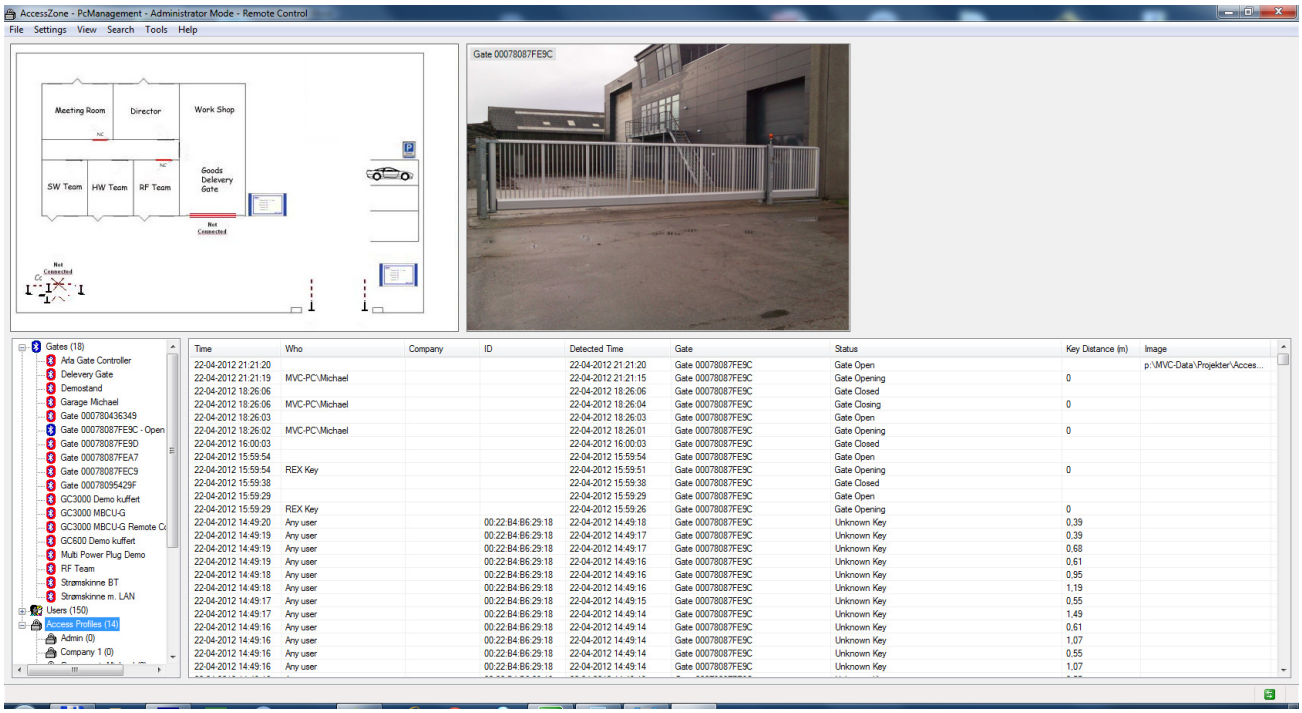
Enter the administrator PIN code if used or leave empty and click ”OK”. Max. up to 16 characters.

If ”Cancel” is selected it stays in ”Operator Mode”.

From Administrator Mode you can switch by clicking menu "Switch to Operator Mode..." from the "Settings" menu or by clicking Ctrl+O to lock for further changes.

4.3 Main Screen

The image below shows how the main screen is organized.



The upper left screen shows a customized overview image (e.g. a CAD drawing) of the secured area or building. You can freely make your own drawing of the secure area/building. The overview image can be enabled/disabled (option).

The different door, barrier and gate symbols can also be customized and be placed freely anyway on the overview drawing. The symbols are automatically updated according to the status events for all the connected GateControllers. I.e. is the door/barrier/gate open or closed etc.

You can design an overview image which looks like the real environment to ease identification of the user accesses and other events.

To the right video images can be shown from a freely selected folder on the PC or server for each GateController™. The images are automatically updated to show the latest image. I.e. it can be images from surveillance cameras at the location. The system administrator can then get a visual indication of the last access as well. This can be enabled/disabled.

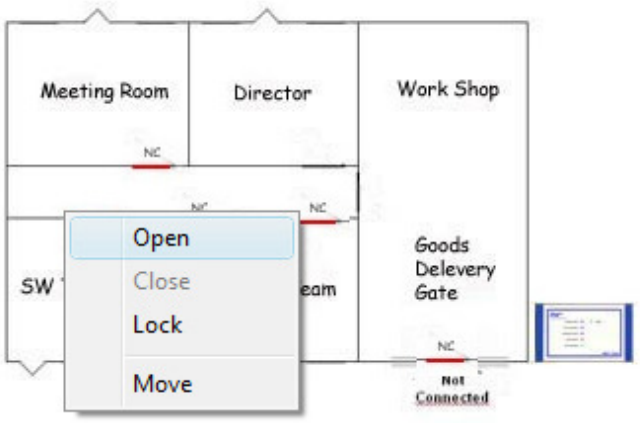
The bottom half shows an event log for all detected users and other events in real time.

Bottom left shows a list with all the controlled GateControllers. Below a list of all registered users (SBD-keys) for easy maintenance and last a list with all the profiles and the users associated with each profile for an easy overview.

General!

A feature must be enabled for a GateController™ and for a user before it becomes active. I.e. this makes it possible to enable a feature for a GateController™ and then specify whatever the feature is going to be used for each user. And a feature can be permanently disabled for all users by disabling the feature for the GateController™ etc.

4.4 Manuel Control of Door, Barrier or Gate



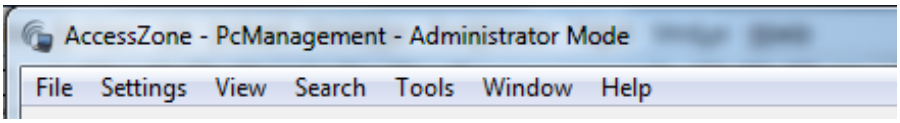
It is easy and fast to control a door, barrier or gate directly from the graphical user interface.

Simply right-click on a door/barrier/gate symbol on the customized image (CAD drawing) of the secured area and then open/close or lock it manually - easy, quick and intuitive.

The desired command is sent to the selected GateController™ which executes the command and sends back a status event.

The graphical symbols are updated to show current door/barrier/gate status. You can also edit the settings for the selected GateController™.

4.5 Main Menu Overview



4.5.1 "File"

This menu contains the "Exit" function to terminate the program. The program can also be terminated with (Ctrl + X)

4.5.2 "Settings"

This menu contains two functions ”Access” (Ctrl+A), Critical Zones (Ctrl+C) and ”Program” (Ctrl-P)

4.5.2.1 "Settings" –> "Access"

Add new users, edit properties for exiting users or delete users. Setup an access profile or edit/delete an exiting profile. This can also be done from the graphical user interface to the left.

4.5.2.2 "Settings" –> "Critical Zones"

Setup a critical zone or edit/delete an exiting critical zone. Menu must be enabled in config.xml file parameter: <config id="Enable Critical Zone" value="1" />

4.5.2.3 "Settings" –> "Program"

To setup some basic program settings controlling how the system operates and enabling of administrator PIN code. Setup of area views, Notifications and remote control for enabling server options. Other settings are handled in the configuration config.xml file.

4.5.2.4 "Settings" –> "Switch to Admin Mode..." / "Switch to Operator Mode..."

To switch between Administrator Mode and Operator Mode witch restart of PcManagement. If Administrator password is applied it must be entered to switch to Administrator mode:

- **Administrator Mode** - changes can be made to users and configuraton

- **Operator Mode** - changes are prohibited

4.5.3 "View"

This menu contains check boxes for adjusting the horizontal displayed event information in the real time monitor window. Click information on and off regarding door/gate entries (Opened, closed or locked). The information is always stored in the system database for later analysis.

The system log (Ctrl+L) shows system status and events. This information is also written in the log file (typical path c:\ProgramData\AccessZone\log\PcManagementLog.log)

4.5.4 "Search"

This menu contains the "Access Log" function. Here you can specify your search filters and search through the database of stored accesses and other events. It can also be started by pressing the "F3"-key.

4.5.5 "Tools"

This menu provides access to the two tools "Firmware Upload" and "Replace GateController".

4.5.5.1 "Tools" –> "Firmware Upload"

The "Firmware Upload" tool is used to upload new firmware to the systems. Refer to the "Firmware Upload User Manual". PcManagement™ must be closed to run this tool.

4.5.5.2 "Tools" –> "Replace Gate Controller"

The "Replace Gate Controller" tool makes it easy to exchange a GateController™. I.e. all the settings and profiles are copied to the new GateController™ and the old GateController™ can be removed.

4.5.6 "Windows"

This menu provides access to area views (if specified) and different log functions:

- Alarm message (F12) Alarm window with active alarms.

- User Status (Ctrl+U) Status information about the users. When was they last detected.

- Gate Controller log (Ctrl+L) Events from the GateControllers e.g. connection time.

- Remote log (Ctrl+L) Information about connected remote - and alarm clients.

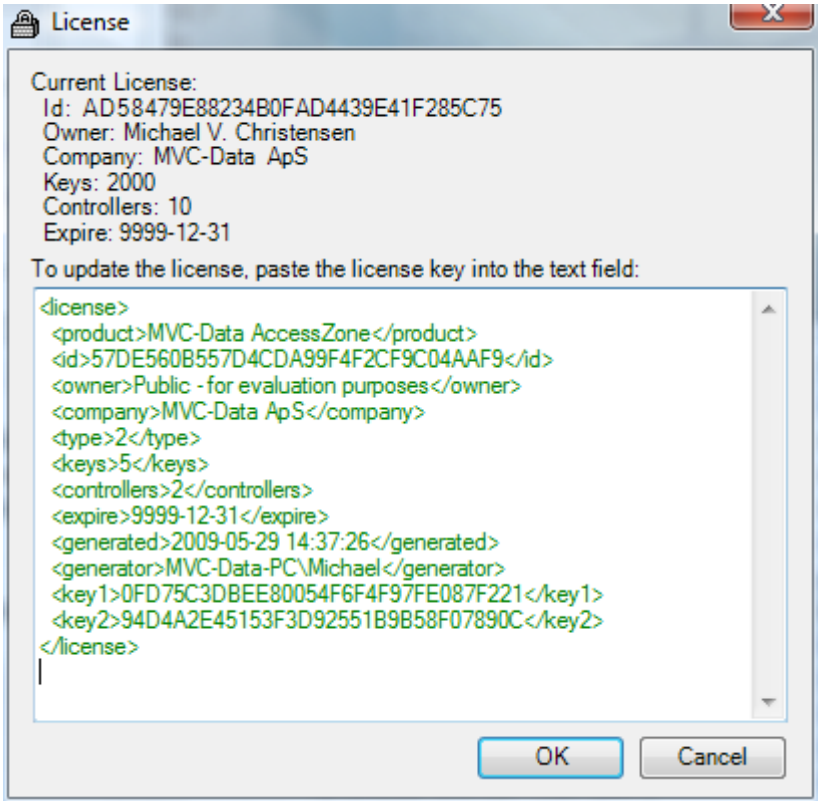
4.5.7 "Help"

This menu contains two functions "License .." for handling the license file and an "About…" box with system information (license information and running time)

4.5.7.1 "Help" –> "License"

This option contains the license function for Copy Past of the license information.

Copy the license information from your purchased license file and past it into the text field.

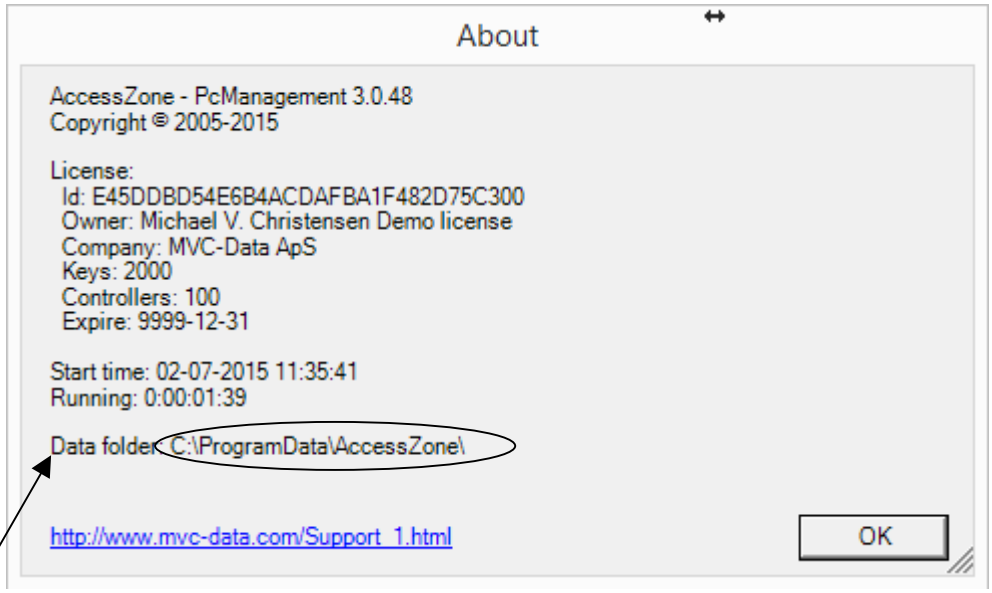


Click OK to store the license.

Please restart PcManagement™ to allow it to activate the new license.

4.5.7.2 *"Help" –> "About"*

This option contains the about box function with system information: PcManagement™ version, license information (ID and rights etc.), started time and the folder path where user program information is stored and a link to a support web page to locate more information (updates).



This is the path to the program data folder (typically a hidden folder) where the configuration data is stored.

Check the "About" box for your system. It may differ and depends on the used Windows version.

4.5.7.3 *Back-up of System Configuration and User Data*

The "Data folder" shown above contains the user data files:

- AccessZone.SQLite.db the database with user data
- config.xml system settings

TIP!
It is recommended to take regular backups of this folder to a backup media for easy restoring of your system in case of a PC break down etc.

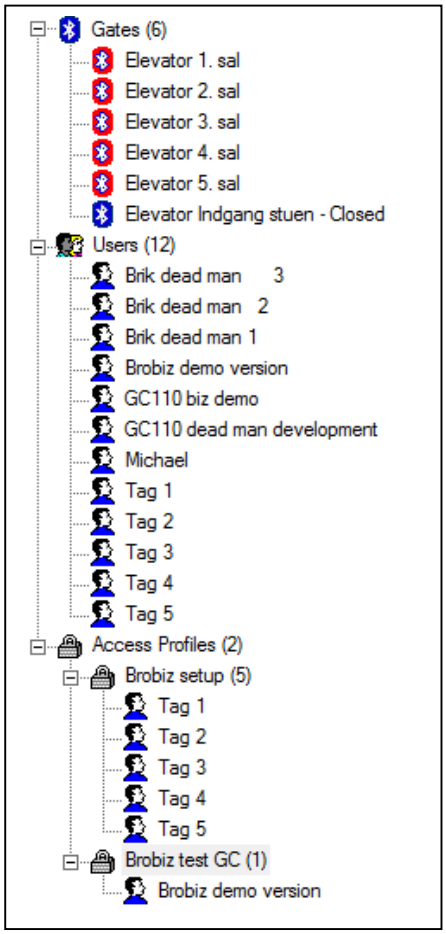
You can also move your system to another PC by restoring these files in the new "Data folder". The files are typically stored in c:\ProgramData\AccessZone\ and can be copied to the same location on the same PC or on a new PC. I.e. all your settings and users are moved to the new PC.

1) First install PcManagement on the new PC.
2) Start PcManagement to setup file folders etc.
3) Close PcManagement
4) Copy your system files from the old PC to the data folder on the new PC
5) Restart PcManagement
6) Your system is now moved to the new PC or restored

4.6 Main Three List Menu Overview

Normal maintanance functions like adding, editing or deleting GateController, users and access profiles are accessable from the main menu. However, most daily maintanance functions are available directly from the GUI by a few clicks on an item in the three list menu to the left of the main window.

The different items in list can easily be expanded or closed to improve the overview:



A list with all the GateControllers in the system.
Blue - Gatecontroller is onlie.
Red - GateController is offline

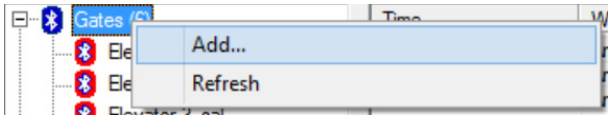
A list with all the users in the system

A list with all the access profiles and a sub user lists with users using the different access profiles

4.6.1 Gates - List with all GateControllers

4.6.1.1 "Gates"

Righ click on top level "Gates" to added or refresh menu list:

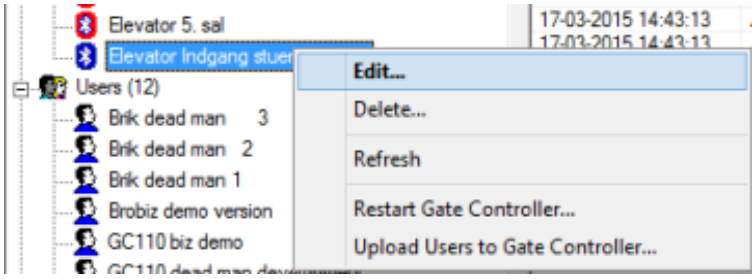


Select:

"Add"	To manually add a new GateController. You must know the unique ID of the new GateController
"Refresh"	Update the menu list

4.6.1.2 "GateController Name"

Righ click on a GateController name to access some maintanance functions:



Select:

"Edit"	To change settings for that GateController
"Delete"	Remove the GateController from the system
"Refresh"	Update the menu list
"Restart Gate Controller"	Some GateController settings e.g. change the "Key Distance" parameters requires the GateController to be restarted to let the new values take effect. Use this to make a restart fo this GateController only. Restart PcManagement to restart alle GateControllers in the system
"Upload Users to Gate Controller"	to make a complete user upload to this GateController only. This could be usefull if upload failed.

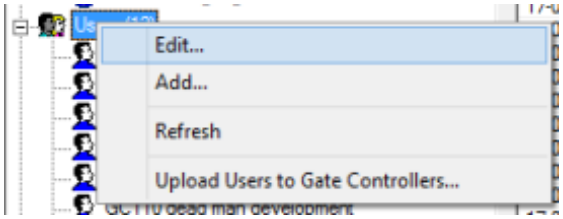
TIP!

Double click a GateController name to open edit menu

4.6.2 Users - List with all the Users

4.6.2.1 "Users"

Righ click on top level "Users" to access user maintanance functions:



Select:

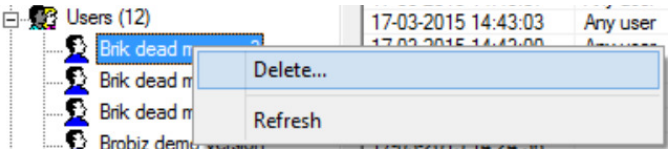
"Edit"	Open "Users" menu to edit users
"Add"	To add a new user. Opens an empty user dialog menu
"Refresh"	Update the menu list
"Upload Users to Gate Controllers"	to make a complete user upload to all online GateControllers at the same time.

Note!

The system will automatically restart a single user upload to a GateController with an invalid user database in case of an faulty update.

4.6.2.2 "User Name"

Righ click on a user to access user maintanance functions:



Select:

"Delete"	Delete the user selected
"Refresh"	Update the menu list

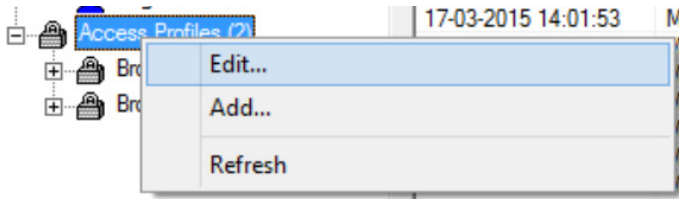
TIP!

Double click on a user name to edit settings for that user

4.6.3 Access Profiles- List with all Access Profiles

4.6.3.1 "Access Profiles"

Righ click on top level "Access Profiles" to access access profile maintanance functions:

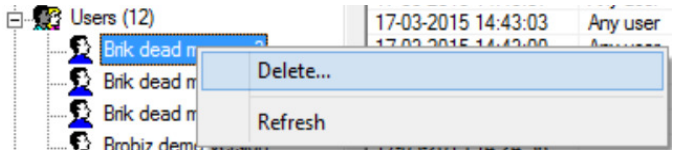


Select:

"Edit"	Open "Access Profile" menu to edit profiles
"Add"	To add a new profille. Opens an empty profile dialog menu
"Refresh"	Update the menu list

4.6.3.2 "Access Profiles Name"

Righ click on a access profile name to access profile maintanance functions:



Select:

"Delete"	Delete the access profile selected **Make sure that no users are using the profile before delete**
"Refresh"	Update the menu list

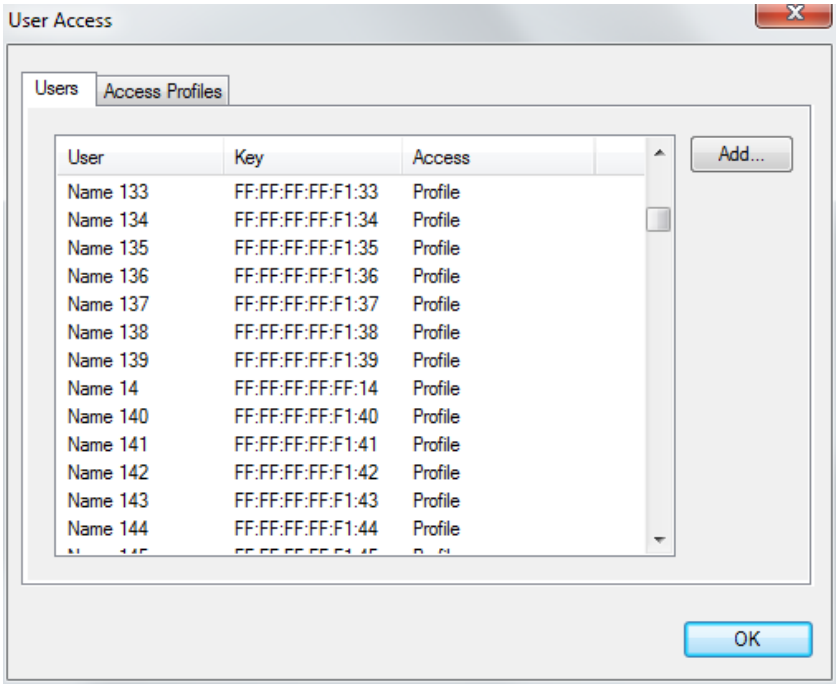
TIP!

Double click on a access profile name to edit settings for that profile

4.7 Menu “Settings” - > “Access” -> “Users”

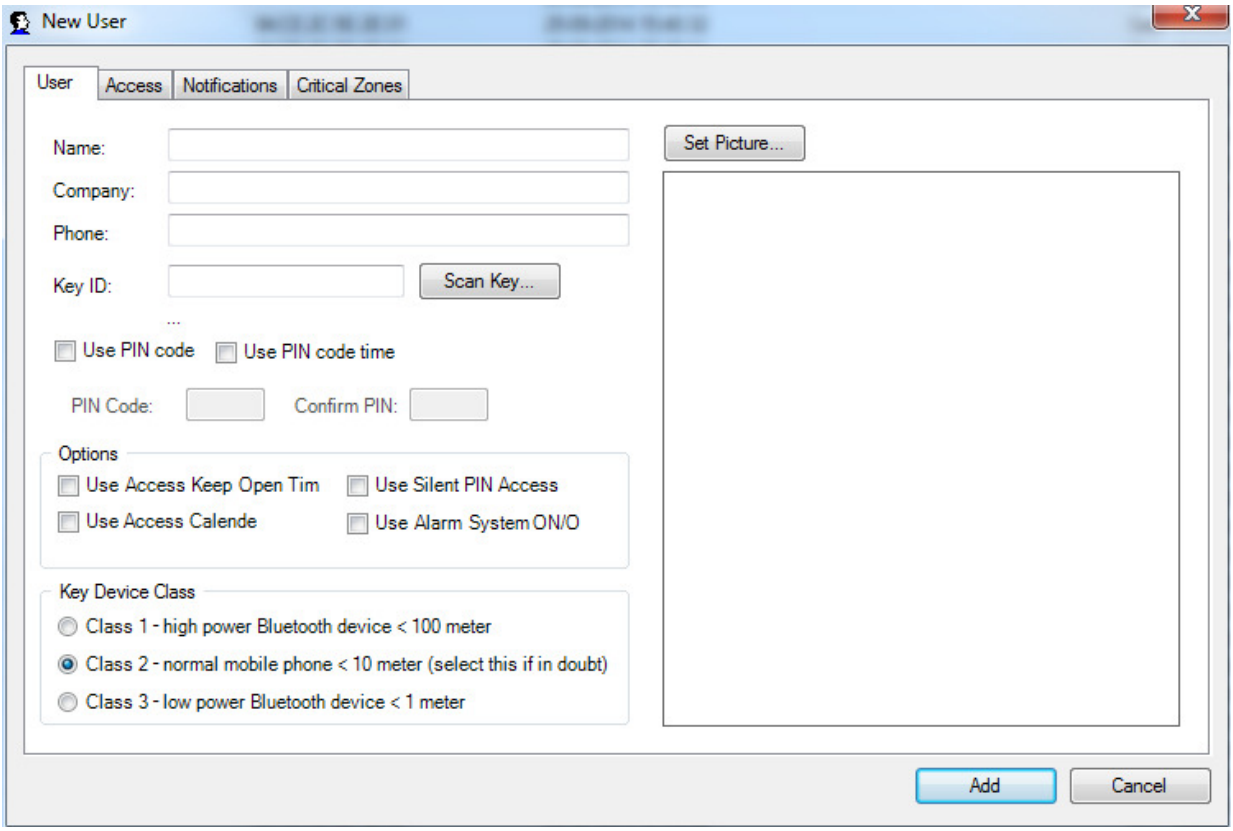
This menu shows all users and their access rights.

Click Add to add a new user or click on an exiting user to edit options or delete the user.



4.7.1 Add a new User – Menu "Settings" - > "Access" -> "Users"-> "Add"

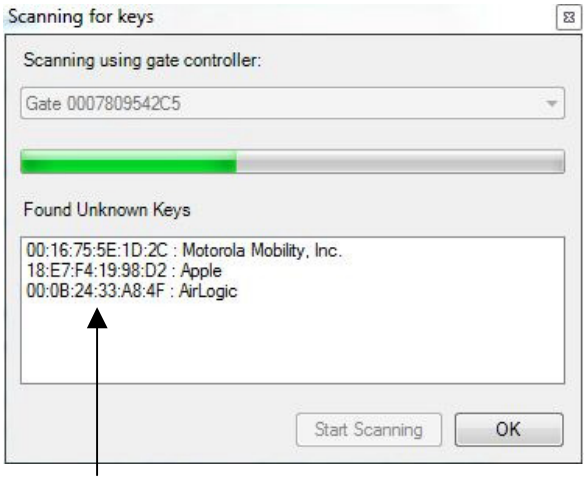
This menu shows the "New User" form to fill out for the new user.



First enter the name of the user and relevant "company" information. The "Company" field can also be used to save additional information about the user e.g. company name of employee or employment group for the user etc. You can also add a phone number and select "Set Picture" to add a picture of the user.

The unique BD address (user ID) of the user's mobile phone or other Bluetooth enabled device can be manually entered in the "Key ID" field or select "Scan" to automatically scan for the user's unique BD address.

The view below shows the system while it automatically scans for new users (SBD keys). The scanning is started manually by clicking the "Scan" button. The detected user IDs (SBD-Keys) and manufacture names (E.g. Apple for iPhones) are listed as they are found:



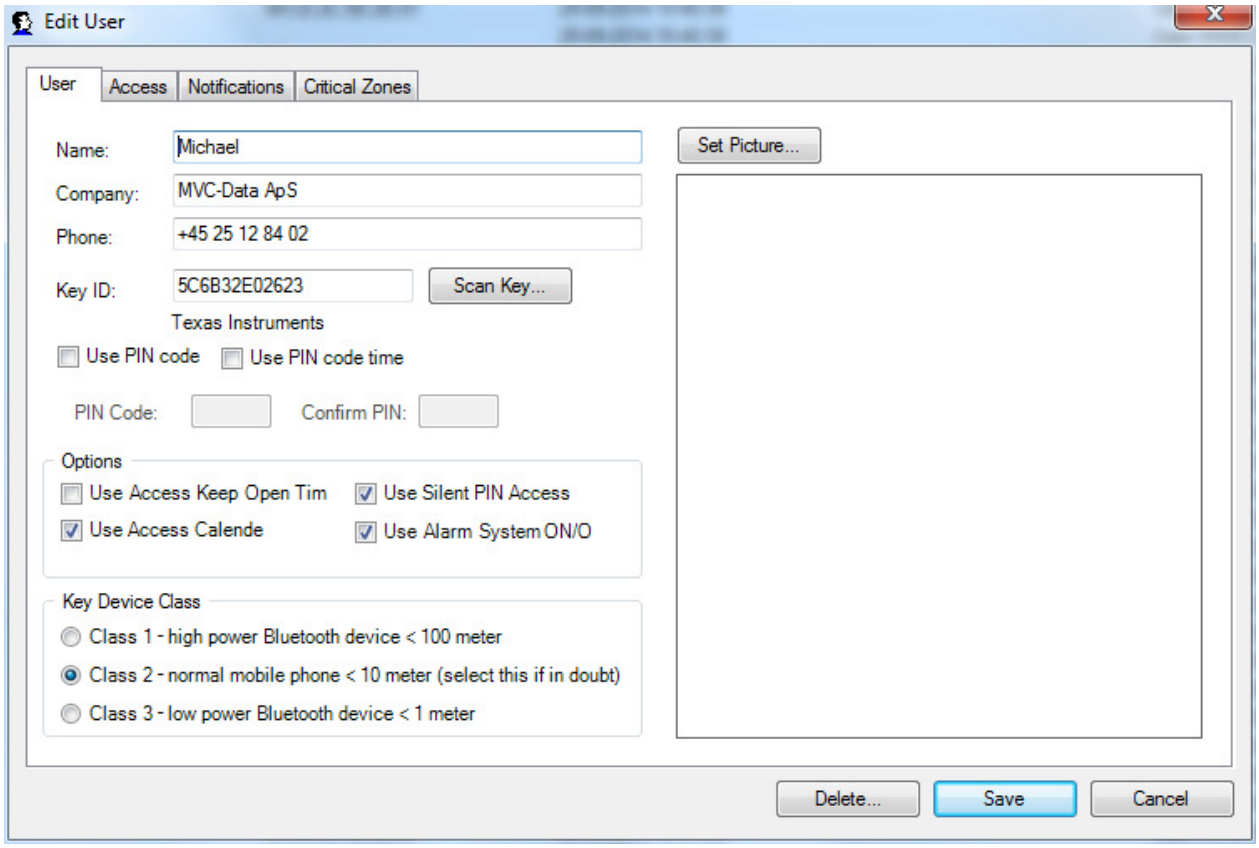
Unique user IDs

When the Key ID is found, mark it in the list and click "OK"

Note!
Any GateController™ can be used to scan for devices. Click the drop down menu to select the desired GateController™

It is recommended to use a specific GateController™ with a short detection range to avoid lists with many detected keys.

Settings and access rights are filled out for the user:



Select whatever the user must use PIN code to get access or just within a specified PIN code time. The PIN code time can be the same or set differently for each GateController™. I.e. PIN code may be required at different times depending on the GateController's location in the system.

Select which options the user must use (no options are selected by default):

- "Use Access Keep Open Time" will allow the user to keep the door/gate open within the specified time period
- "Use Access Calendar" will enforce the user to comply with the GateController calendar
- "Use Silent PIN Access" will allow the user to enter a special "silent" access PIN code. The user must type the PIN code 4 times to activate. The door/gate will be open as normal but an alarm is trigged in the system to alert system administer/security personal
- "Use Alarm System ON/OFF" will allow the user to switch an alarm system ON and OFF

Last select the device power class for the user (device):
Class 1 = "strong device" Class 2 = "standard device" Class 3 = "weak device"

If a user's device must be closer to the reader than most others before access is granted
- select class 3 = "weak device".

If a user's device gives access further away from the reader than most others
- select class 1 = "strong device".

Click "Add" to add the user or "Cancel" to leave without adding the user.

TIP!
A mobile phone is typically a class 2 device. If you are in doubt select Class 2 (default).

Remember a feature must also be enabled in the GateController™ for it to work.

4.7.2 Add a new User – Virtual Key pad – Menu "Settings" - > "Access" -> "Users"-> "Add"

The system supports a virtual keypad feature which can operate in two different modes: Virtual Key Only Mode and Virtual Keypad Mixed Mode

This feature will allow access to all users that know the 4 digit access PIN code.

4.7.2.1 Only Mode

The system can be configured to run as a purely virtual key pad. I.e. no specific users have to be added.

Common keypad:
The system administrator adds a "user" with the special BD address "FFFFFFFFFFFF" (not a valid BD address) and the desired 4 digit access PIN code. This "user" and access PIN code is the same for all GateControllers™ in the system.

Individual keypad:
The system administrator adds a "user" with the special BD address "FFFFFFxxxxxx" (not a valid BD address). "xxxxxx" is the GateControllers lower address part, in example with 00078043633F xxxxxx = 43633F and can be found in the "Info" box. And the desired 4 digit access PIN code for this particular GateController. I.e. this "user" and access PIN code is specific for the GateController™ specified.

The system will in this mode grant access to all users which enter the correct 4 digit virtual keypad access PIN code.

The PIN code can be disabled if "0000" is used as PIN code and thereby give access to all with a Bluetooth enabled device – a simple gate/door opener.

TIP!
The system administrator can at any time change the PIN code. E.g. on a daily or weekly basis.

4.7.2.2 Mixed Mode

The system can also be configured to be in mixed mode virtual key pad with up to the system limit minus 1 (number of supported users depends on the license acquired) of unique users and a virtual keypad user with the special common BD address "FFFFFFFFFFFF" or individual BD address "FFFFFFxxxxxx" and the 4 digit access PIN code.

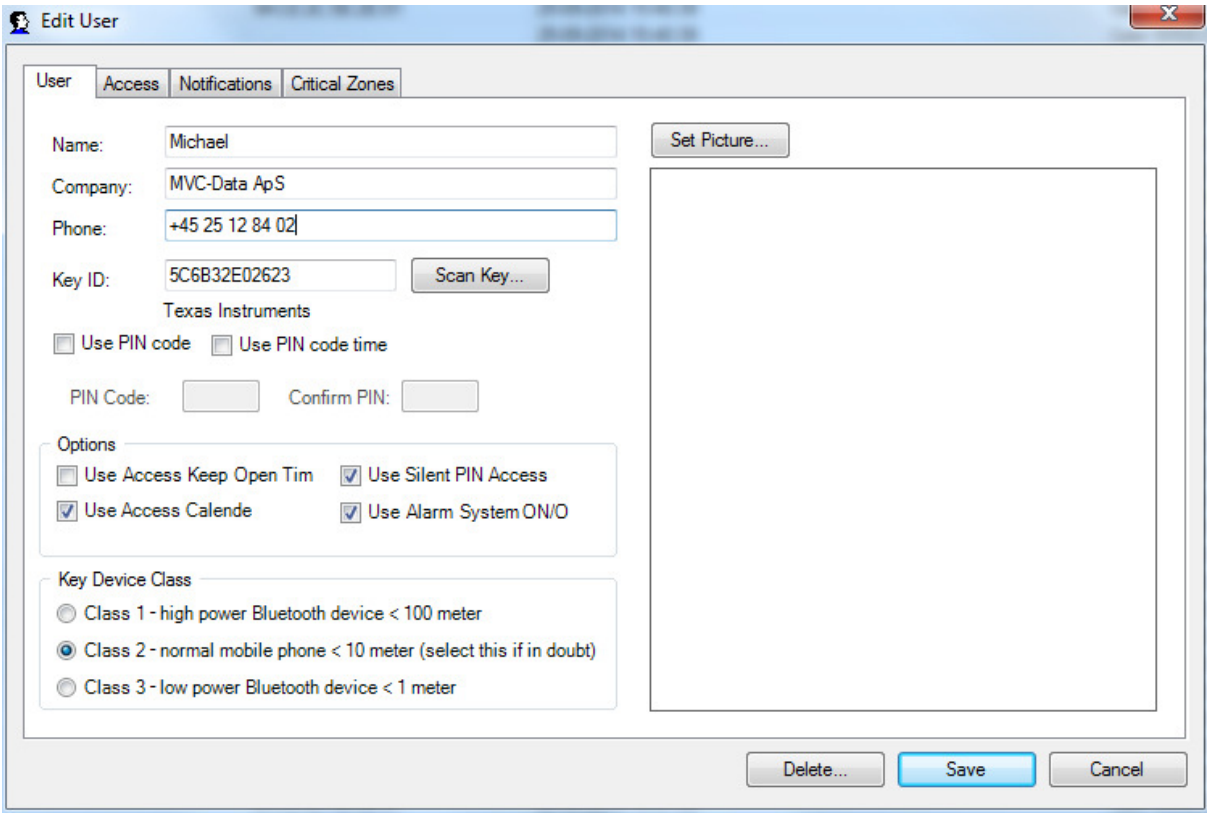
The system will in this mode grant access to all individually added users with or without a unique 4 digit access PIN code and to all other unknown users which enter the correct 4 digit virtual keypad access PIN code.

TIP!
This feature allows the virtual keypad PIN code to be changed without affecting all the individually added users.

The common virtual keypad can be combined with the individual keypad "user" on selected GateControllers. If both the virtual keypad "user" and the individual "user" are used with a GateController - the individual PIN code is used.

4.7.3 Edit or Delete User – Menu "Settings" - > "Access" -> "Users"- "User"

Click on an existing User in the list to make changes to the user settings:

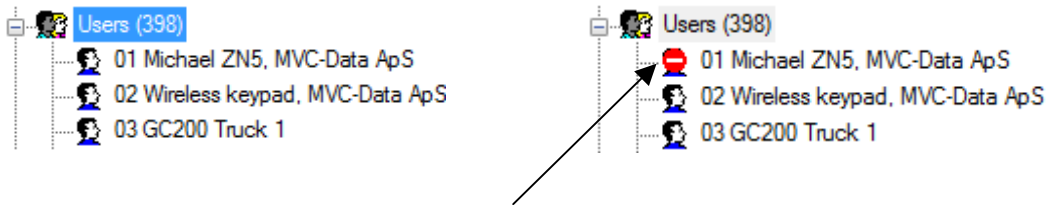


Edit the user settings. Select "Access" or "Notifications" to make further changes:

- Save: Click "Save" when done to store the new settings
- Delete: Click "Delete" to completely remove the user from the system
- Cancel: Click "Cancel" to leave the menu without making any changes

TIP!
A user can be temporally disabled from the system in case of a lost user key (mobile phone) by setting the users access permission to "Block All Access". The user will be detected but no admission will be allowed. The system must be online to update the GateControllers. The access event attempt is still logged in the database and an email notification can be send. Please refer to *User Acceess Profile*

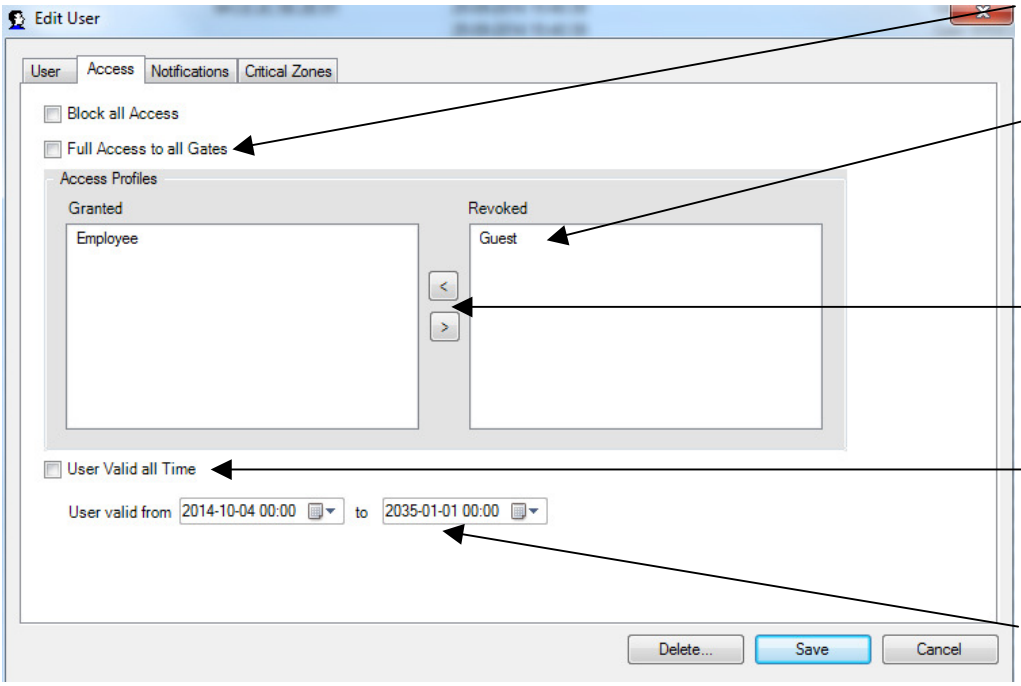
You can also select the users directly from the drop down list shown on the graphical user interface to the left by double clicking on a user:



User is now temporally blocked

4.7.4 User Acceess Profile – Menu "Settings" - > "Access" -> "Users"- "Access"

This view shows the menu for specifying the access rights for the new user. You can select multiple profiles for each user:



Click "Full Access to all Gates" or select an access profile from the list.

"<" to add or ">" to remove the selected access profile

Remove the mark to enable booking feature.

Enter the start - and end date and clock for the user.

- "Block All Access" select to (temporarily) block all access for a particular user
- "Full Access to all Gates" select to allow full access disregarding any time profiles on all doors/barriers/gates. This profile should only be used with a limited number of users. This is the default setting
- Select an access profile. Remove all markings from "Block All Access" and "Full Access to all Gates" to select from the list of access profiles. One or more access profiles can be selected. Click the '<' symbol to add the access profile or '>' symbol remove the access profile

Booking Option:
Remove the mark from "User Valid all Time" (default) to allow the user to be enrolled after the calendar. I.e. the user can be added now but first be enrolled at a later date. A user also be enrolled and automatically be removed at a specific date without further interaction.

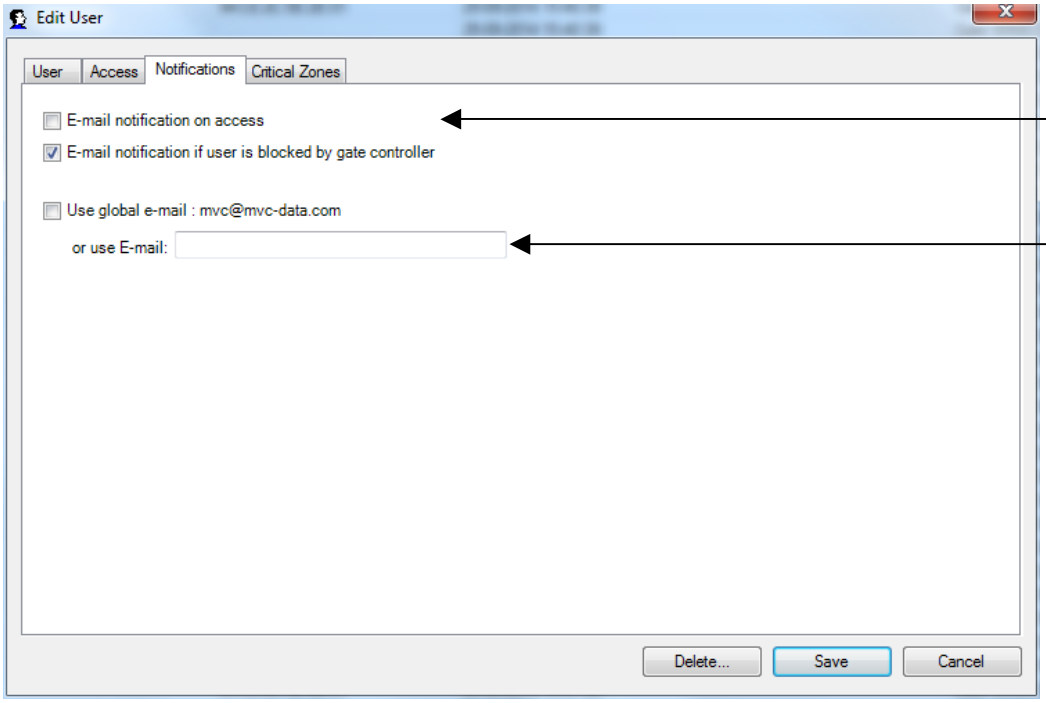
Note! Booking is only working with online GateControllers.

Edit the user access settings. Select "User" or "Notifications" to make further changes.

- "Save" when done to store the new settings
- "Delete" to completely remove the user from the system
- "Cancel" to leave the menu without making any changes

4.7.5 User Acceess Notification – Menu "Settings" - > "Access" -> "Users"- "Notifications"

This view shows the menu for specifying the email notification to send for all access for a particular user:



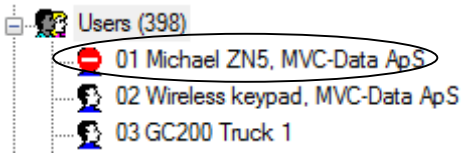
Click a notification to enable it.

Specify to use a common email address or enter a unique email address for that particular user

- "E-mail notification on access" select if an email notification is required on all access for that particular user
- "E-mail notification if user is blocked by gate controller" select if an email notification is required in case the system blocks that particular user for any further accesses.

  This could be the case if the user has entered the 4 digit access PIN code wrong 3 times in a row. System administrator must then remove the "Block All Access" marking for the user to allow access again. See section *User Acceess Profile*.

  The user will be marked as blocked in the user list to the left:

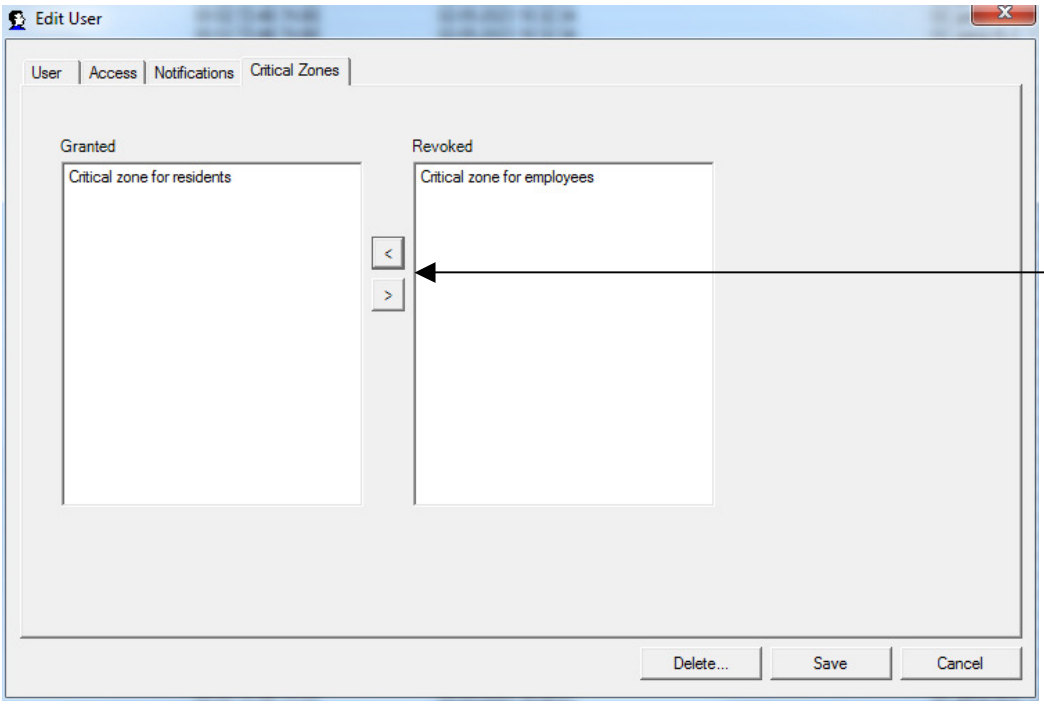


- "Use global email" specify whatever the global email account should be used to send the event or specify a custom one for that particular user

Edit the notification settings. Select "User" or "Access" to make further changes and click "Save" when done to store the new settings.

4.7.6 User Acceess Notification – Menu "Settings" - > "Access" -> "Users"- "Critical Zones"

This view shows the menu for specifying different critical zones which can be used by one or more users:



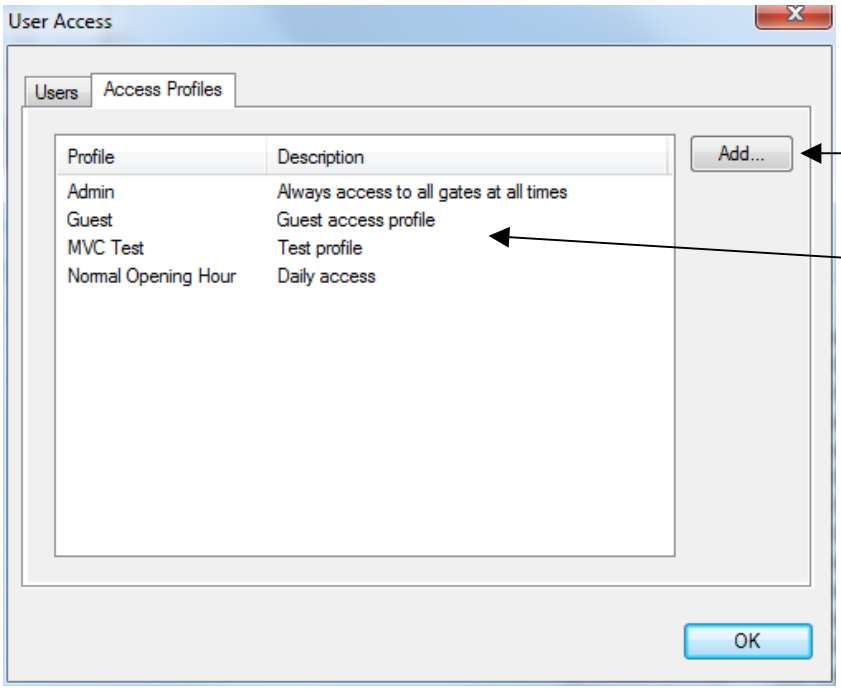
Click a critical zone to enable it.

"<" to add or ">" to remove the selected critical zone

More critical zones can be enabled for a user.

4.8 Menu “Settings”-> ”Access” -> “Access Profiles”

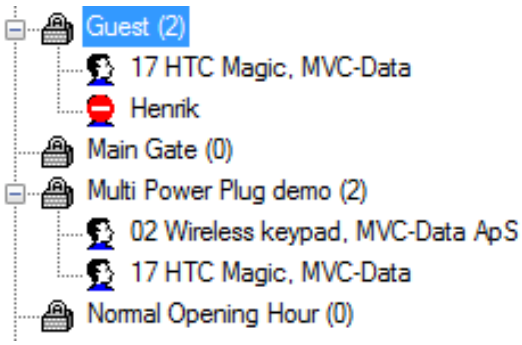
This view shows an overview of the exiting Access Profiles.



Click “Add” to add a new access profile or click on an exiting access profile to edit the options or to delete it.

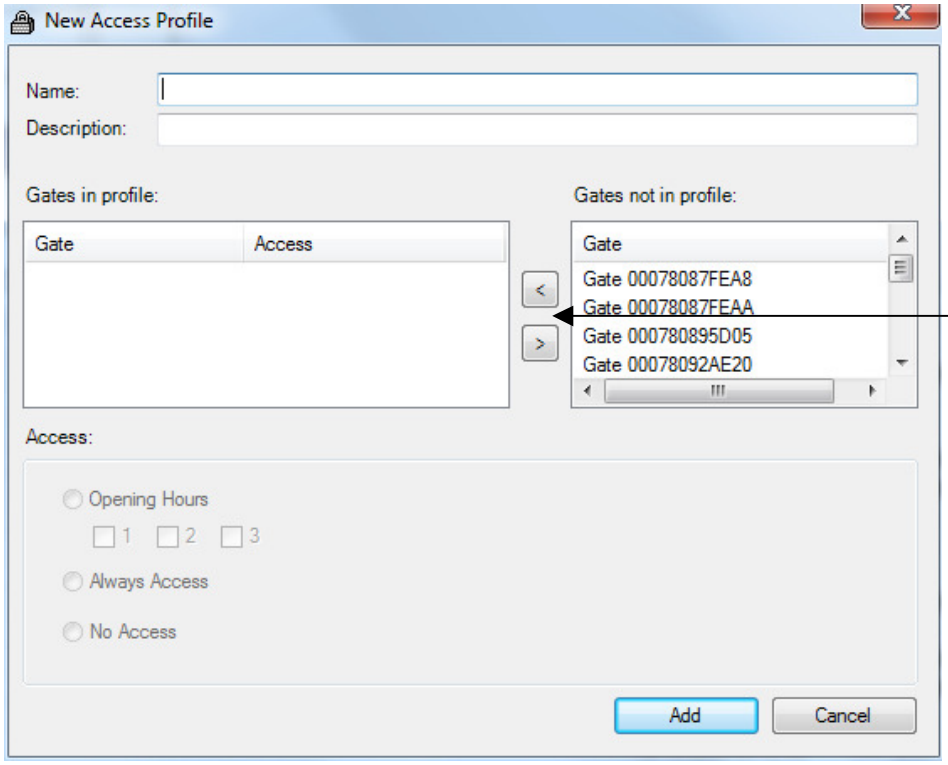
Click “OK” when done.

The access profiles can also be selected directly from the graphical user interface to the left. It also shows which users who use the profile:



4.8.1 Add a new Access Profile – Menu "Settings" - > "Access" -> "Access Profiles" –"Add"

This view shows the new Access Profile menu. This menu can also be open by right clicking on the "Profile" drop down list in the graphical user interface to the left.



Click "<" to add or ">" to remove the selected GateController

- "Name" specify the profile name
- "Description" write a short description to make it easy to understand the purpose of the Access Profile
- "Gates in profile" select all the doors/gates to use with that Access Profile
- "Gates not in profile" use the '<' or '>' to add or remove doors/gates from the Access Profile
- "Access" specifies the time profile to use in the Access Profile for each of the selected GateControllers in the Access Profile. Click "Opening Hours" to select any combination e.g. 1 and 3 or 1 and 2 etc. of the defined time profiles or "Full Access" or "No Access" (blocked mode)

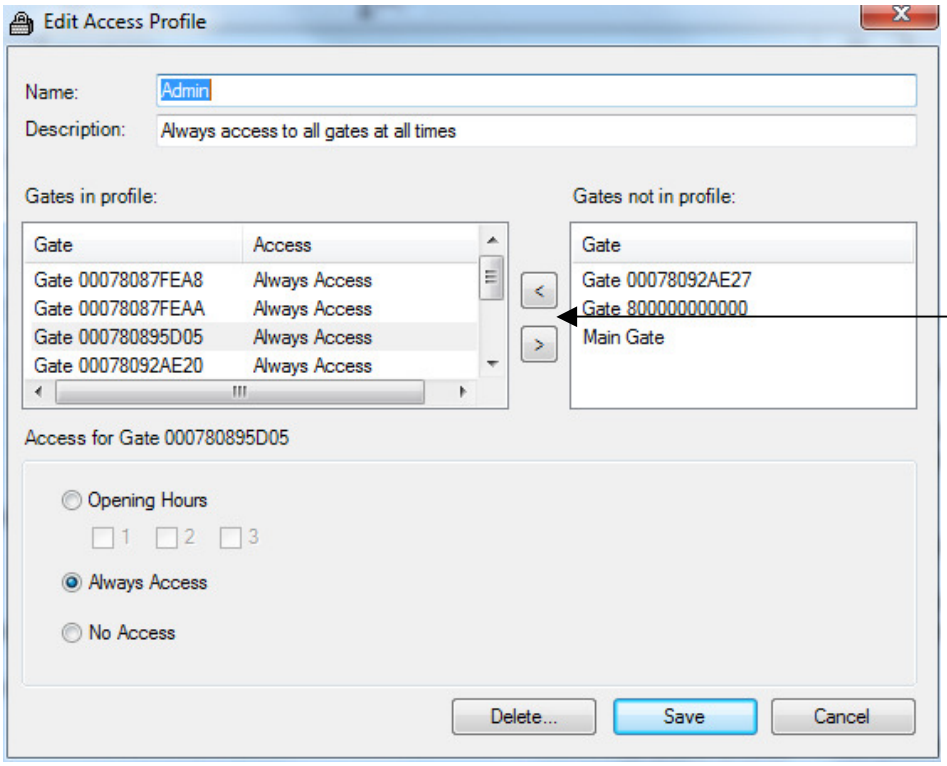
  Note!
  The time profiles may differ between GateControllers depending on user selection. Refer to section 4.11.1 *Time Profile - Menu "Opening Hours"*

Click "Add" to store the new Access Profile. Click "Cancel" to leave without changes.

TIP!
Remember to add a new GateController™ to new and any existing access profiles as required allowing the profiles to work with the new GateController™.

4.8.2 Edit or Delete a Access Profile – Menu "Settings" - > "Access" -> "Access Profiles"

This view shows an existing Access Profile menu. This menu can be open by clicking on an existing Access Profile or by right clicking on the access profile in the drop down list in the graphical user interface to the left.



Click "<" to add or ">" to remove the selected GateController

Edit the access profile and click "Save" to store the changes or click "Delete" to remove the access profile from the system.

- "Edit" change the access profile settings. Click "Save" when done to store the new settings
- "Delete" to completely remove the access profile from the system

  Caution!
  It is highly recommended to remove an Access Profile from the users before deleting it.

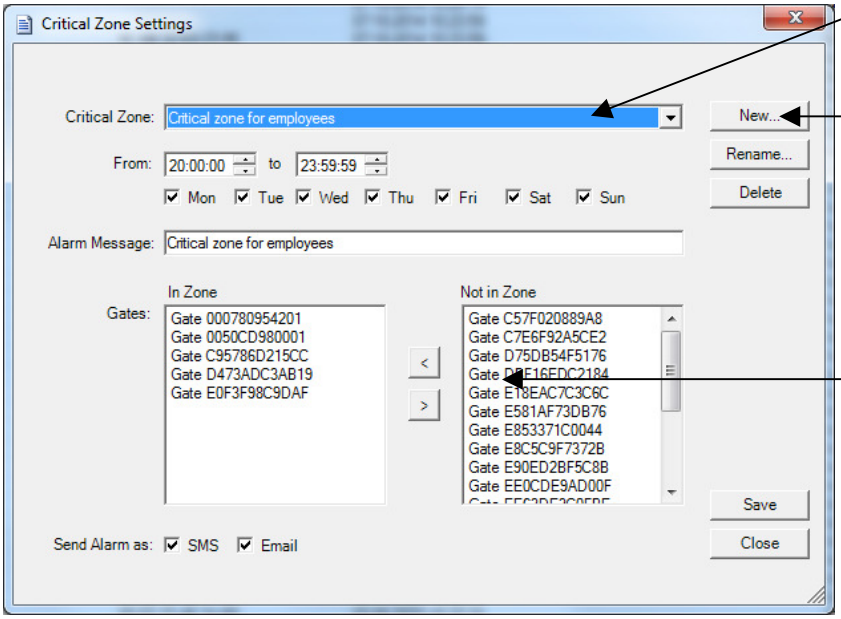
  Make sure that the users have another valid Access Profile

- "Cancel" to leave the menu without making any changes

4.9 Menu “Settings”-> ”Critical Zones”

A critical zone is an detection area where you can get an alarm if a user moves into the zone in the specified time interval. The feature is normally used within elder care to warn if a resident is trying to get out of a door in the evening or night. However, it can also be used to warn security personal that a user is still within the area(s). I.e. the area should have been empty e.g. at a construction site.

This view shows an overview of the critical zones.



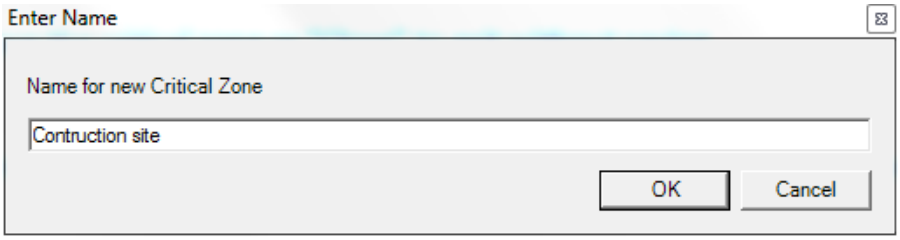
Click on an existing critical zone to edit

Click ”New” to make a new critical zone

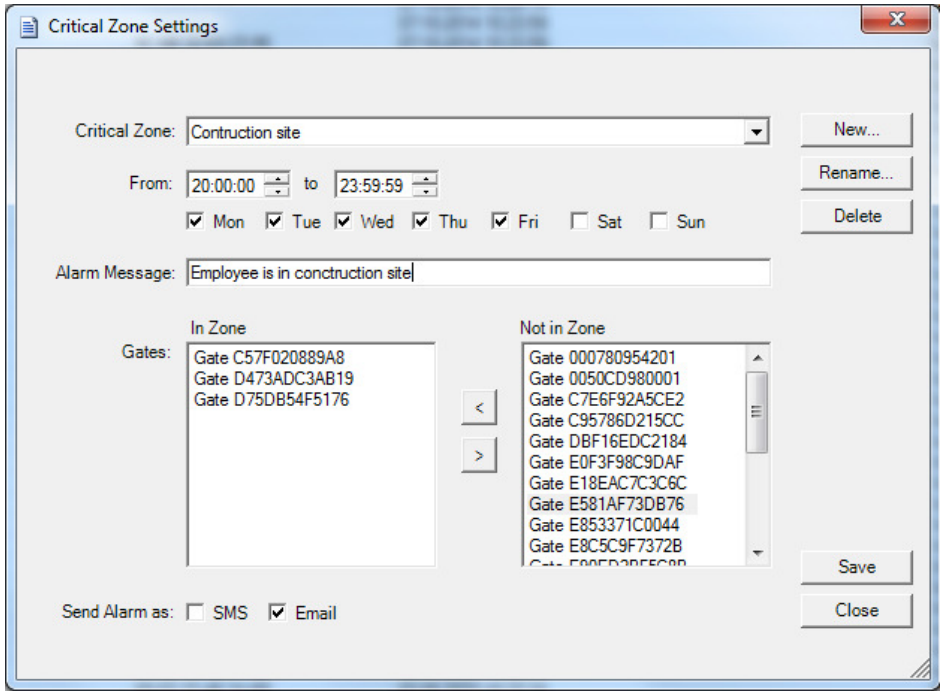
Click ”<” to add or ”>” to remove the selected GateController

Click “New” to define a new critical zone or click on an exiting critical zone to edit the options or click "Delete" to delete it.

4.9.1 *Add a new Critical Zone:*



- Click “New" and enter a name for the new location - remote group and click "OK"



- "From:" select the time period and weekdays where the alarm must be active

  Note!
  You can only enter time within one day. I.e. from 00:00:00 to 23:59:59

  If you need a zone covering evening and night you must split the zone into two zones. E.g. The first zone "Evening" covers from 20:00:00 to 23:59:59 and the second "Night" covers 00:00:00 to 08:00:00.

- "Alarm Message" enter the text to send

- "Gates" select the GateControllers covered in this critical zone "In Zone".

- "Send Alarm as" specify how the alarm is send: As SMS and/or Email.

  TIP!
  For SMS refer to section 4.10.4.1 Notification as SMS

- Click "Save" when done.

TIP!
The Critical zones must be selected (enabled) for the users under "Critical Zones" under "Edit User"

4.9.2 Delete or Rename Critical Zone:

Select a Critical Zone in the list and click "Delete" to delete the critical zone or "Rename" to enter a new name for the critical zone.

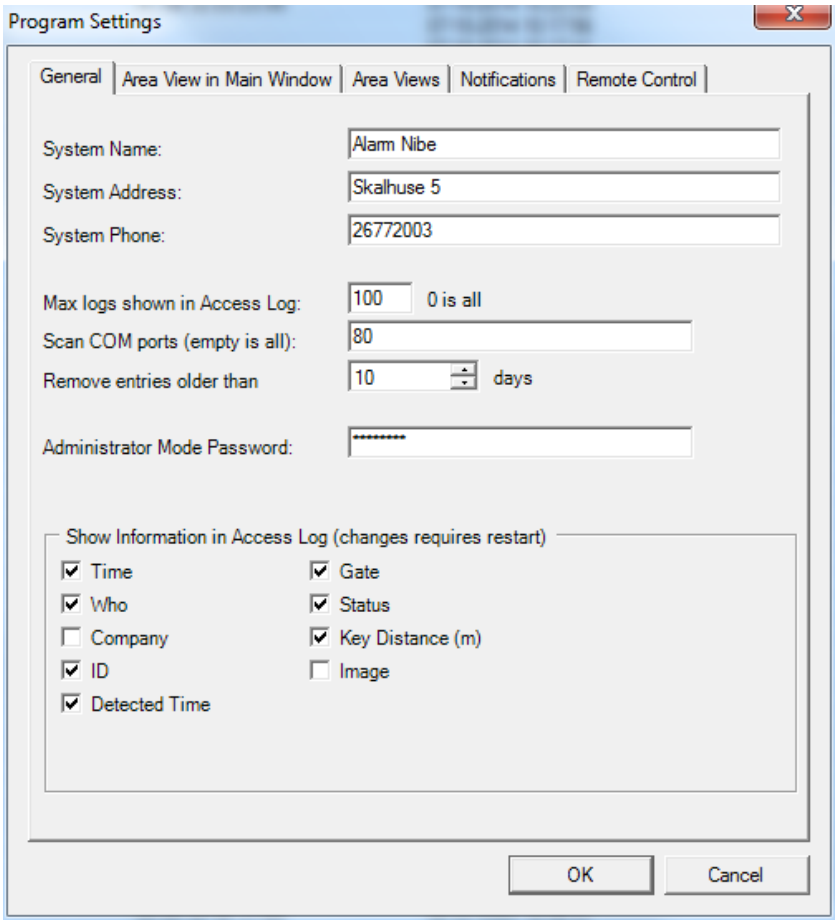
Click "Save" to save a critical zone or "Close" to exit without saving.

4.10 Menu “Settings”-> ”Program Settings”

This menu can be located in the main menu “Settings” “Program” or directly by activation of (Ctrl-P)

4.10.1 General Settings - Menu “Settings”-> “Program Settings” – “General”

Menu for the general system settings:



- "System Name" enter a name for the server to make it easy to identify when using alarm clients
- "System Address" enter the address of the location of the server
- "System Phone" enter a telephone number for clients to call for support
- “Max logs shown in Access Log” specifies how many logs shown in the main screen. If set to 10 only the 10 newest events are shown. All events are still stored in the database for later analysis. Default is 1000
- “Scan COM ports (empty is all)” specifies all the COM ports the system must search for a GateController™. The list is ‘,’ (comma) separated. This is important if the PC running the PcManagement™ system contains COM ports which are not connected to a GateController™. E.g. COM port 2, 4, 6 and 8 is specified like this “2,4,6,8”. Default is empty

Note!
LAN/Wi-Fi and Bluetooth connected devices must also be mapped to a COM-port:

Bluetooth setup refer to: AccessZone Bluetooth Setup Manual

LAN setup refer to: AccessZone XPORT Setup Manual

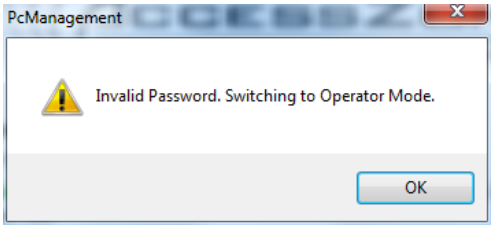
Wi-Fi setup refer to: AccessZone_GC3000_WiFi_Module_Setup_Manual

- "Remove entries older than" specifies how old the event log data are. I.e. when they will be automatically deleted. Default is 90 days

- "Administrator Mode Password" specify an administrator PIN code to be used when starting the system. Max. up to 16 characters.

  If PIN code is enabled:
  - PcManagement™ can only switch to "administrator mode" if the PIN code is correct entered.

  - If the PIN code is not entered it stays in "operator mode". GateController™ and settings cannot be changed in "operator mode" – Events can be viewed.



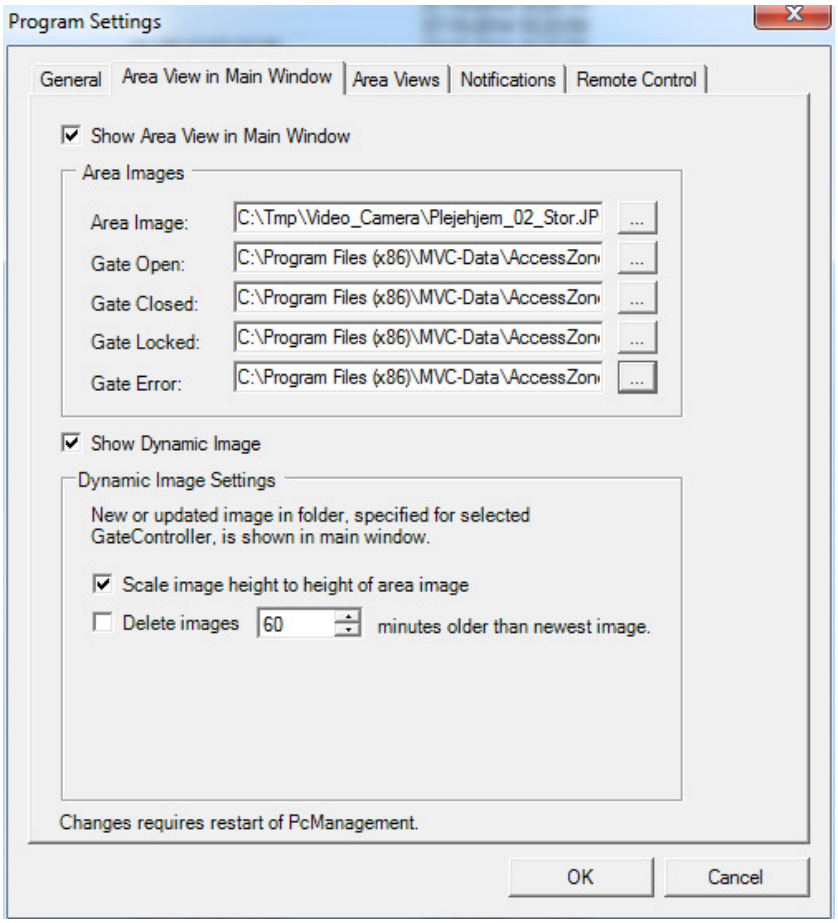
  - Erase the PIN code field to completely disable the administrator PIN code. I.e. it is possible to startup in "administrator mode" without entering a PIN.

  If PIN code is disabled:
  - PcManagement™ is always started up in "operator mode". Use Ctrl+M and "Yes" to switch to "administrator mode" and Ctrl+O and "Yes" to switch back to "operator mode".

- "Show Information in Access Log" to enable/disable information shown in the main screen window. E.g. if "Key Distance (m)" information is not important it can be hidden from the main screen window for a simpler overview. Default is all enabled

4.10.2 Images - Menu "Settings"-> "Program Settings" – "Area Views in Main Window"

Menu for specifying the different images to use as area image and a default door/barrier/gate symbols for open, closed, locked and error state. The images are default and are used if no images are specified for a GateController™:



- "Show Area View in Main Window" select if you want a image (CAD drawing) shown of the secured area in the main window.

  Enter the path and filename for the area image and gate symbols to place on the area image.

  TIP!
  You can use an "Area View" instead of the area view in main window to get more space for event logs.

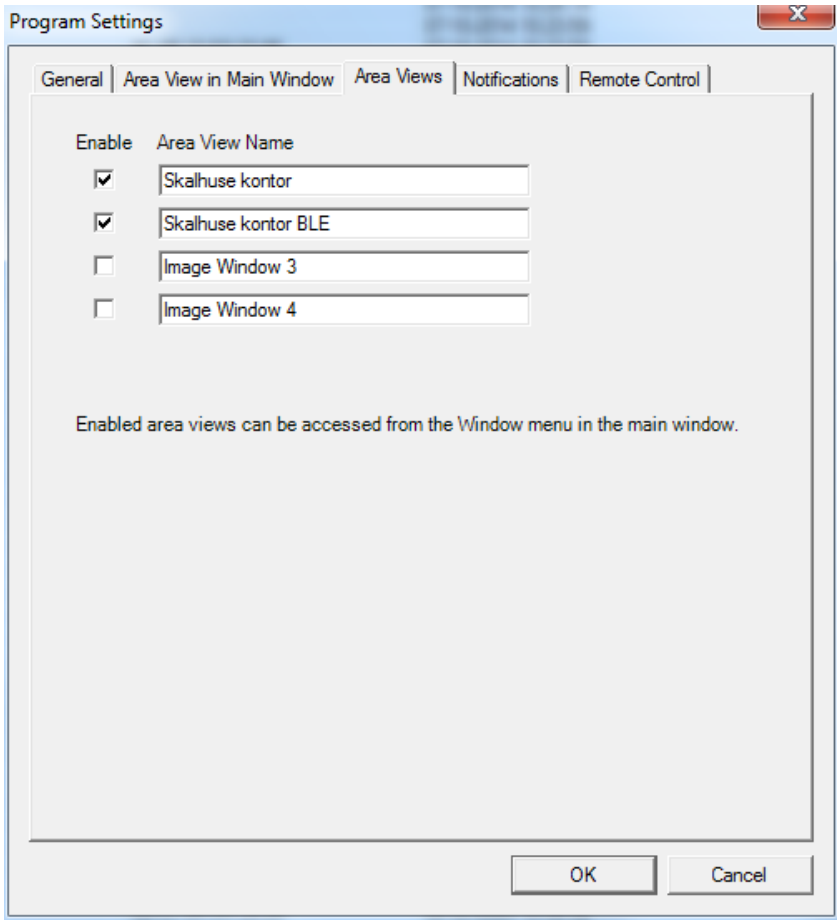
- "Show Dynamic Image" select if you want images from a surveillance camera shown to the right of the area image. It can be freely selected from any folder on the PC or server. The image is automatically updated and shows the latest image. Specify whatever the images must be scaled to fit area image and if the images must be automatically deleted

  TIP!
  The shown image will be tagged with the access open event to make it easy to locate the image.

Click "OK" when done or click "Cancel" to leave without changes.

4.10.3 Notifications - Menu "Settings"-> "Program Settings" – "Area Views"

Menu for setting up the area views:



You can define up to 4 area views which can be shown as separate images with PcManagement in minimized state

- "Enable" set a mark to enable the area view
- "Area View Name" enter a name for the area view to make it easy to identify

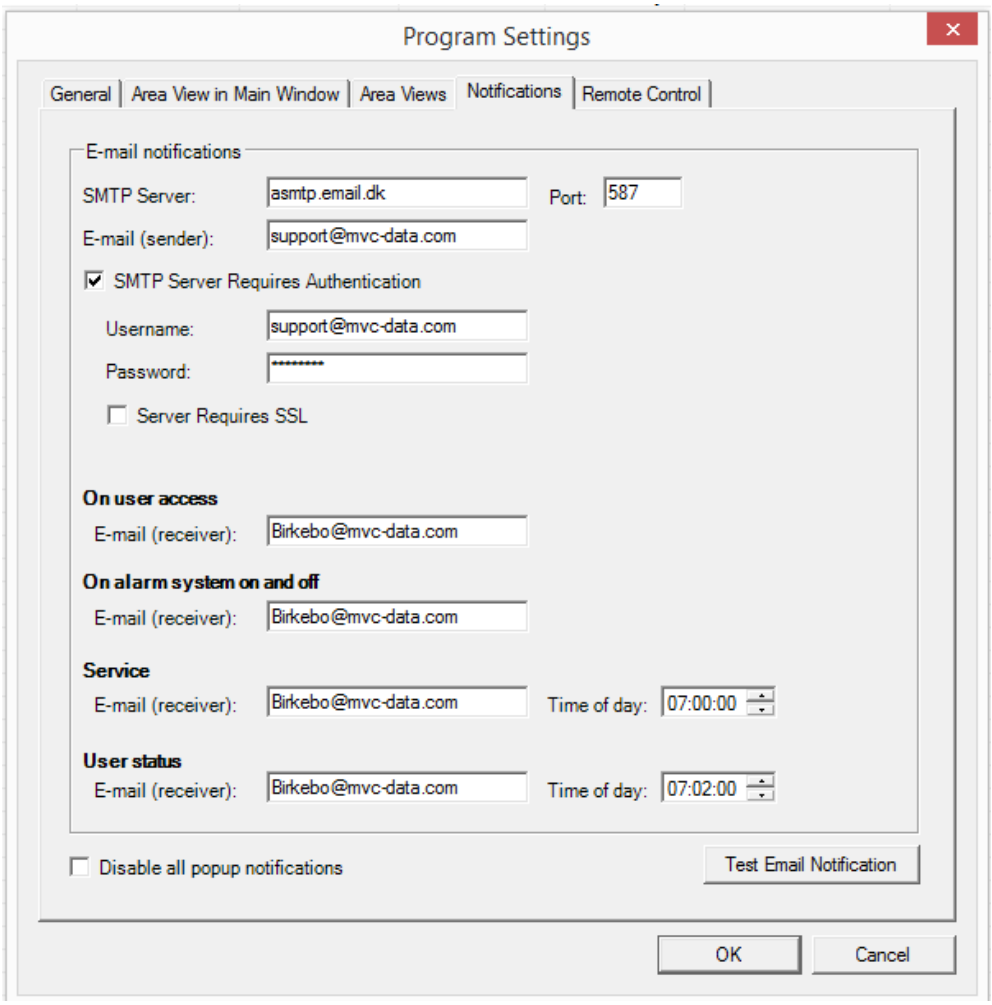
Click "OK" when done or click "Cancel" to leave without changes.

TIP!
The gates to show on the area view must be specified in the area view.

The area views can be activated from the main "Window" menu.

4.10.4 Notifications - Menu "Settings"-> "Program Settings" – "Notifications"

Menu for the general system email notifications setup:



Note!
The PC running PcManagement™ must have an internet connection to use this feature.

Email server setup:

- "SMTP Server"
  Specify your SMTP server and port number (default is 25). The SMTP server to use depends typically on the internet provider you have. Check your normal email program or ask your network administrator

- "E-mail (sender)"
  Specifies the e-mail address to use as the sender for the e-mails

- "SMTP Server Requires Authentication"
  Set a mark if the SMTP server requires a user name and password.

- "Server Requires SSL"
  Set a mark to enable SSL.

Email setup:

- "On user access"
  "E-mail (receiver)" specifies the e-mail address to send to on user access events

- "On alarm system on and off"
  "E-mail (receiver)" specifies the e-mail address to send to when the alarm is armed (on) or disarmed (off) or for general alarm messages like nurse call, security call etc.

- "Service"
  "E-mail (receiver)" specifies the e-mail address to send maintanance and service information from the system to the maintanance and service personal or company.

"User Status"

- "E-mail (receiver)" specifies the e-mail address to send a daily user status report with notifications on "not seen" since the last daily report (> 24 hours) and low batt. warnings marked with red.

Email with daily user status report

User Status

2015-07-02 07:05:02

MVC-Data ApS
Skalhuse 5
+4525128402

#	User	Additional Info	ID	Current Location / GC	Current Key Distance	Previous Location / GC	Time	Button Status	Battery Status	Batt %	Acc Status	Temperature
1	Test BIZZ 2	FW 094 med diode	5C313EDAB3D1	Kontor COM 11 / C95786D215CC	-65dBm [3,90m]	Kontor COM 11 / C95786D215CC	2015-07-02 07:00:51	0x00	OK	94	00	19
2	Test BIZZ 3 | + 45 25 12 84 02	FW X94	5C313EDAC83E	Lab COM 10 / FAC40C1773DF	-70dBm [6,19m]	Lab COM 10 / FAC40C1773DF	2015-06-24 13:04:06					
3	Morten	MVC-Data ApS	94CE2C5E2E01	Lab COM 10 / FAC40C1773DF	-77dBm [11,79m]	Lab COM 10 / FAC40C1773DF	2015-06-25 19:37:12					
4	Test BIZZ 1	FW 094 med diode	5C313EDABE4C	Kontor COM 11 / C95786D215CC	-79dBm [14,17m]	Kontor COM 11 / C95786D215CC	2015-07-02 06:56:20	0x00	OK	94	00	20
5	MVC Test brik	FW X94 uden DC DC	5C313EFAA17C	Kontor COM 11 / C95786D215CC	-70dBm [6,19m]	Kontor COM 11 / C95786D215CC	2015-07-02 07:03:16	0x00	OK	100	00	23
6	Fald demo		5C313EDABE74	Kontor COM 11 / C95786D215CC	-70dBm [6,19m]	Kontor COM 11 / C95786D215CC	2015-06-19 10:49:31	0x00	OK	88	00	18
7	Tryghedskald		5C313EDAC818	Kontor COM 11 / C95786D215CC	-68dBm [5,15m]	Kontor COM 11 / C95786D215CC	2015-06-19 10:50:00	0x00	OK	86	00	22

Click "Test Email Notification" to verify your settings. It will send 4 emails.

Popup notifications:

- "Disable all popup notifications"
  Click field to disable Windows popup notifications with who got access etc.

Click "OK" when done or click "Cancel" to leave without changes.

TIP!
You can send emails to multiple recipients at once by separating the email addresses with a space or comma.

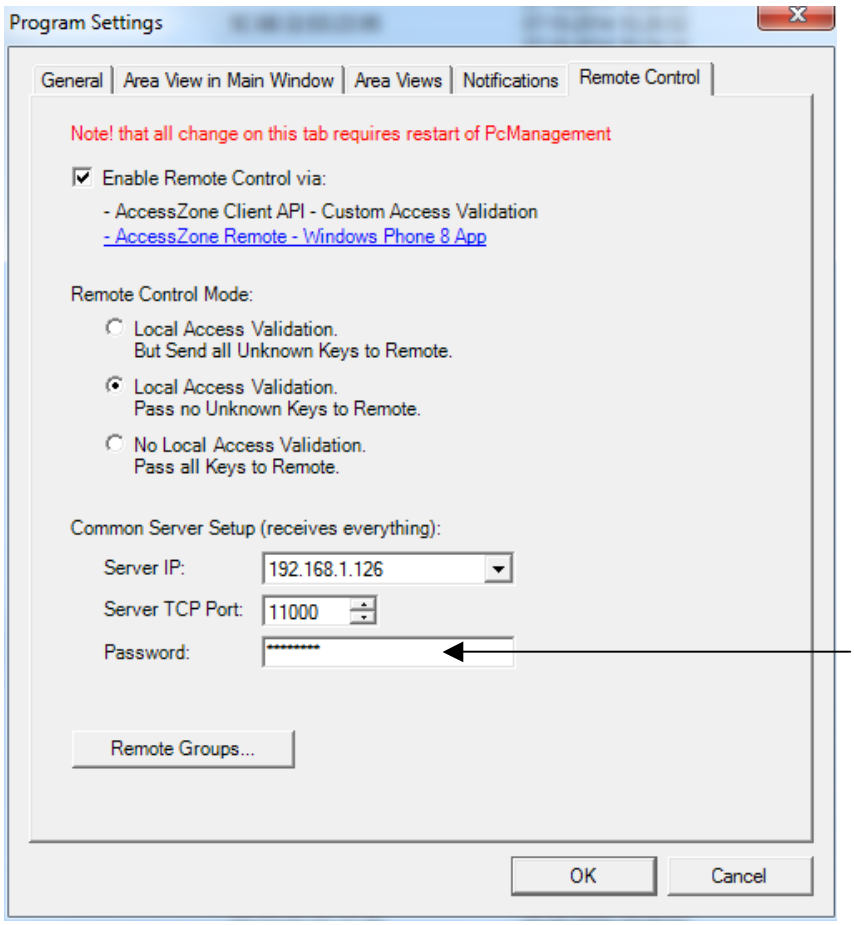
4.10.4.1 Notification as SMS

Emails with alarm messages can also be sent as SMS directly. **However, this requires that a modem supporting SMS-Tunnel (like Moxa) is connected to the PC running PcManagement**.
Configuration is done in the config.xml file:

<config id="SMS Modem Serial Port" value="3" />	Specify the COM port of the modem, e.g. 3
<config id="Send SMS on Safe Alarms" value="1" />	Set "1" to enable, "0" to disable

4.10.5 Notifications - Menu "Settings"-> "Program Settings" – "Remote Control"

Menu for the general system remote control setup:



Enter a unique login password for remote clients. E.g. 37282736

Note!
The PC running PcManagement™ must have an internet connection to use this feature.

The "Remote Control" feature is typically used with the "AccessZone Remote™" client application for remote monitoring and control of the PcManagement server or by the "Alarm Client™" for sending alarms in real time to other PC. However, you can implement your own client with the AccessZoneClient.dll .Net component. Contact us to get the SDK for developing your own application.

- "Enable Remote Control via AccessZone Client API" specifies whatever you want to allow remote control of your PcManagement server.

  Remote Control Mode:
  - "Local Access Validation But send all unknown keys to Remote"
    This option will first make a local validation of the detected users (keys) and allow access if the detected user (key) are valid. Unknown users (keys) are sent to the remote client for validation.

- "Local Access Validation Pass no unknown keys to Remote"
  This option will make a local validation of the detected users (keys) and allow access if the detected user (key) are valid. Unknown users (keys) are skipped.

  Use this option if you only want to monitor and control (open/close and see status) your gates from the Remote client.

- "No local Access Validation Pass all Keys to Remote"
  This option will send all detected users (keys) to the remote client for validation. No local validation in the GateControllers are performed.

  Use this if your own application using AccessZoneClient.dll must validate the users and send open/close commands back to the PcManagement server.

  Caution!
  All menus with user setup are removed from the system

- Network Settings:

  - "Server IP" the IP address of the PcManagement server. I.e. the PC's IP address running PcManagement server.

    TIP!
    It is recommended to use a fixed IP address for the server to avoid that it is accidentally changed.

  - "Server TCP Port" the main TCP server port number. Default 11000

    TIP!
    An Alarm Client can use this port number to get all the alarms from all locations.

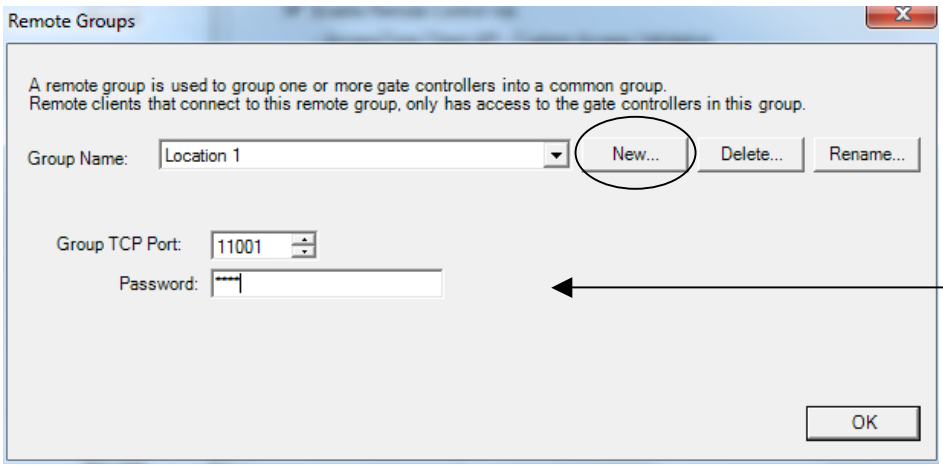
  - "Password" a unique 8-digit login password. The same password must be applied on the remote and alarm client side

Note!
PcManagement must be restarted to allow the changes to take effect.

All communication to remote client is encrypted for secure use.

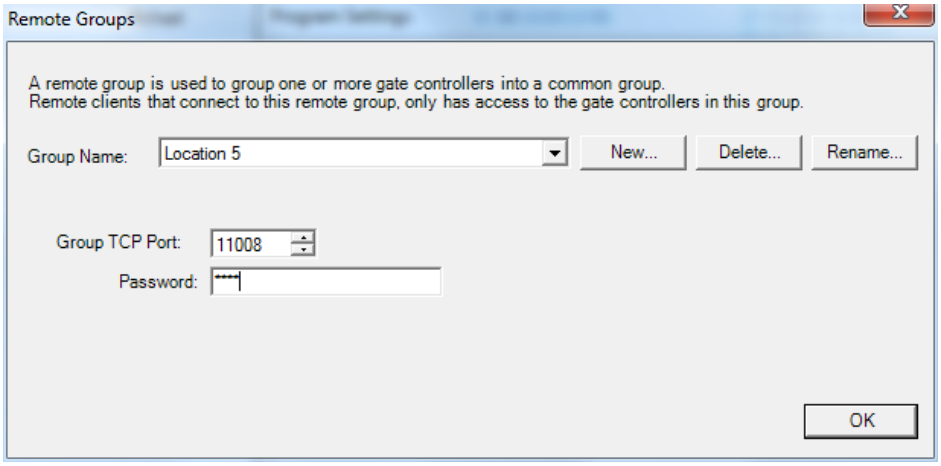
4.10.5.1 Locations - Setup Remote Groups

This view shows how to add, delete or rename location - a remote group.



4.10.6 Add a new location - Remote Group:

- Click “New" and enter a name for the new location - remote group and click "OK"



- “Group TCP Port" enter the port number to use with this location - remote group.
- “Password" enter a login password to secure the communication
- Click “OK"

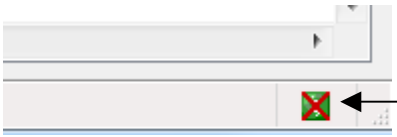
4.10.7 Delete or Rename a location - Remote Group:

Click "Delete" and select a group name to delete or "Rename" to enter a new name for the group.

4.10.8 Remote Client Connection Status

It can always be monitored whatever a remote client is connected from the connection status symbol on the main screen bottom right side.

A remote client is connected



No remote client is connected

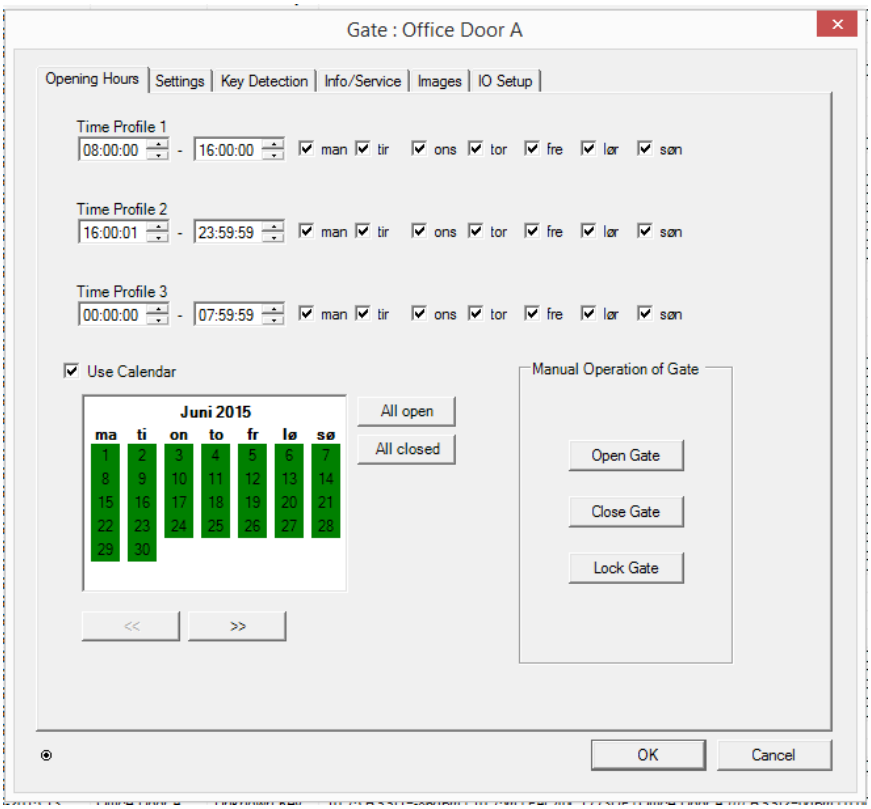
TIP!
Move the mouse pointer over the Client symbol to see how many clients that are connected right now.

4.11 GateController™ Settings –"Gates"

The GateController™ settings are unique for each GateController™ in the system. The menu can be open by right clicking on the GateController™ in the list to the left or directly on the door/barrier/gate symbol on the graphical user interface.

4.11.1 Time Profile - Menu "Opening Hours"

The image shows the menu to setup the opening hours for the GateController™. It is possible to specify 3 different time profiles (intervals) and select which week days access is allowed. These time and day profiles are used when creating the access profiles.



- "Time Profile 1,2 & 3" sets the beginning and ending time and specify which week days the time interval is valid for. The time intervals may overlap

- "Use Calendar" is selected to enable the calendar function for that particular GateController™. A green colour means that access is allowed that day. Mark a date as closed (Red) by clicking on the date. Click again to make the date an normal open day. Click '>>' to go to the next month and '<<' to go back again. It will always show current month and one year ahead making it possible to set open and close days for one year at a time.

  Note!
  The "Use Calendar" option must also be enabled in all the user profiles to make this function work. I.e. if either have this option disabled the feature is disabled. This allows that some users run according to the calendar and others not.

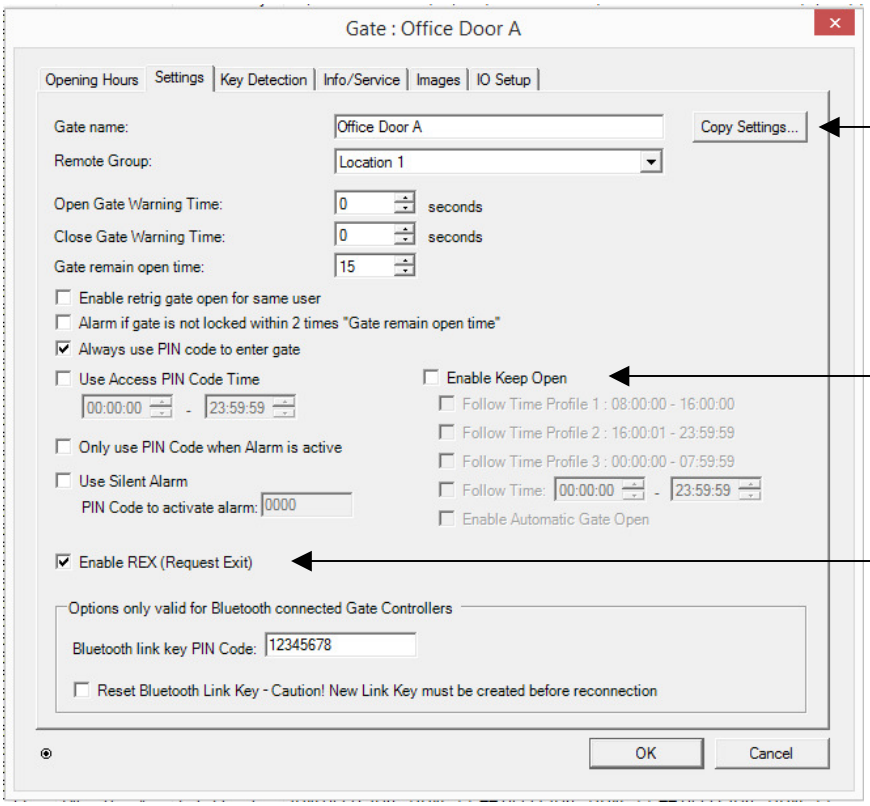
- "Manual Operation of Gate" is used to manually control the door or gate remote. Click "Open Gate" to open the door/barrier/gate etc.

Caution!
The AccessZone® GateControllers with PC interface contain a (real time) clock and date. The clock and date are automatically set and adjusted through the PC connection to PcManagement™. As long as the PC is connected the clock and date are automatically adjusted.

However, if PcManagement™ is closed for a longer period of time the clock may drift a little – the drift is coursed by small drifts in the internal clock frequency and is mainly influenced by temperature variations and component tolerances. I.e. the clock should be updated on a regular basis by reconnecting the GateController™ to PcManagement™.

4.11.2 Gate Settings - Menu "Settings"

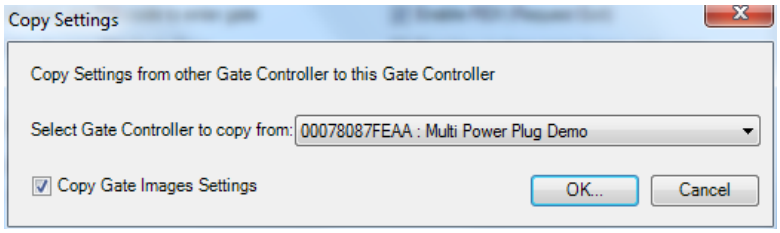
The image shows the menu for some operational settings for the GateController™:



- "Gate name:" give the GateController™ a unique name for easy identification

  TIP!
  The GateControllers are sorted alphabetical in the main screen. Write a number in front of the name to sort the GateControllers as you prefer '1' for the first one etc.

- "Copy Settings" option for copying the GateController™ settings from another GateController™.



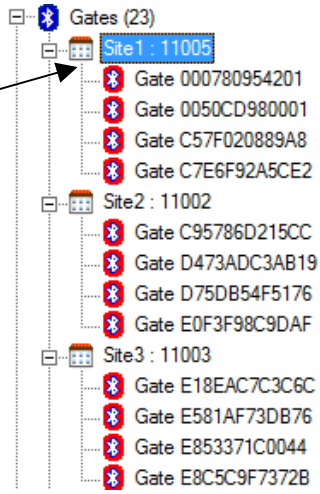
  Select the GateController™ to copy settings from in the drop down list.
  Click "OK" to copy the settings. Use this feature for easy setup of multiple doors and gates.

  Note!
  The GateController™ name and video folder (Menu "Images") settings are not copied.

- "Remote Group" select the location for the GateController.

  The GateController will be listed under the specified remote group name.

  Select <None> if no group must be used with the Gatecontroller.



4.11.2.1 Gate Handling Options:

- “Open Gate Warning Time” specified the number of seconds the buzzer must run before opening the door/barrier/gate. ‘0’ seconds disables warning buzzer. Default is 2s
  Note! Gate opening is delayed with the open warning time.

- “Close Gate Warning Time” specified the number of seconds the buzzer must run before closing the door/barrier/gate. ‘0’ seconds disables warning buzzer. Default is 2s
  Note! Gate opening time is extended with the close warning time.

- “Gate remain open time” the number of seconds the door/barrier/gate as a minimum is kept open. I.e. the delay before closing the door/gate again. Default is 15s
  Note! Gate opening time is delayed and/or extended with the open/close warning time.

- ”Enable retrig gate open for same user” to allow the gate to stay open as longs as the valid user is detected.
  Note! It is recommended to use “Gate remain open time” values above 10 seconds with this feature in RF noisy environments. I.e. heavy Bluetooth and Wi-Fi activity.

- ”Alarm if gate is not locked within 2 x ”Gate remain open time” ” if selected the system will generate an alarm if the door is not closed again as expected.
  Note! The lock must support read-back of the lock state.

4.11.2.2 PIN Code Options:

- “Always use PIN code to enter gate” is selected if an access PIN is required to enter the door or gate. Access PIN must also be enabled for the users to be functional. I.e. both must have this feature enabled. Default is enable.

- “Use Access PIN Code Time” is selected if access PIN code is only required with the specified time interval. E.g. this could be after normal working hours. Access PIN Code Time must also be enabled for the users to be functional. I.e. both must have this feature enabled. Default is disable.

- "Only use PIN Code when Alarm is active" a comfort mode where the access PIN code is only required if the alarm has been enabled. If another user has disabled the alarm by entering the access PIN code the next user isn't prompt for the access PIN code. Default is disable.
  This option requires that one of the PIN code options above have been selected.

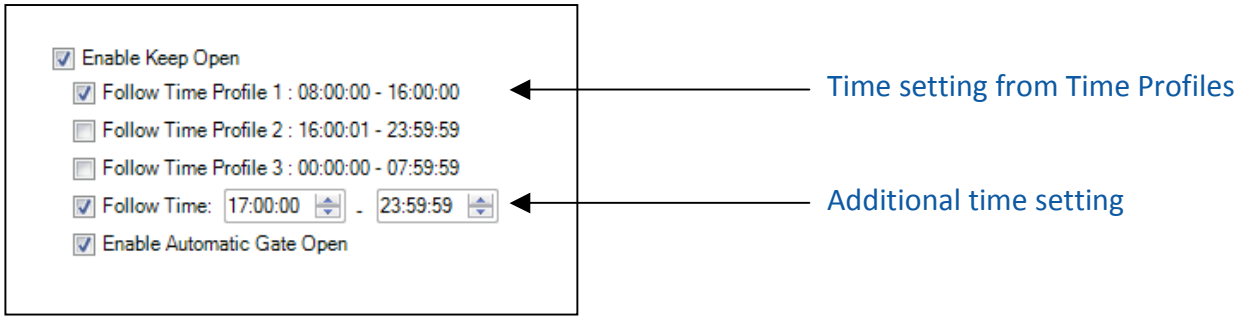
- "Use Silent Alarm" is selected to enable the silent alarm feature. A user can get access when this code is entered 4 times or by 3 wrong PIN codes and then use this PIN code the 4th time. The door/gate is opened and an alarm is triggered and an event is sent to alert the system administrator or security personal. Default is disable.
  This option requires that one of the PIN code options above have been selected.

- "Enable REX (Request Exit)" must be selected to allow use of the REX feature. Default is disable.

4.11.2.3 Keep Open option:

The keep open feature allows the GateController to work as an automatic door/barrier/gate opener. It is well suited for access control to more public areas. It works after the specified time interval either after access has been granted to valid user or full automatically after the time schedule specified.

Note!
The keep open feature follows the settings for weekday access and the system calendar.



- "Enable Keep Open" specifies the time interval where the door/barrier/gate will be kept open from and automatically closed again. Set a mark in the check box to enable feature.

  - Select "Follow Time Profile 1" to use the same time interval as time profile 1
  - Select "Follow Time Profile 2" to use the same time interval as time profile 2
  - Select "Follow Time Profile 3" to use the same time interval as time profile 3
  - Select "Follow Time" to specify a new additional time interval
    Note! This setting does not have a weekday setting

    The first valid user which is granted access will open the door/barrier/gate.

    TIP!
    Select any combination of the 4 keep open time intervals.

- Select “Enable Automatic Gate Open” to automatically open the door/barrier/gate at the beginning of the specified time without any user intervention.

Note!

- “Follow Time Profile 1,2 and 3 are only supported by firmware versions:
  - GC630/GC640/GC670 from version 2.03
    GC3000 from version 1.96

  - Older firmware versions only supports the “Follow Time” option but not the “Enable Automatic Gate Open” feature.

- The “Use Access Keep Open Time” feature must also be enabled for the users to be functional. I.e. both must have this feature enabled. Default is disable.

Options below are only valid for GateController™ using a Bluetooth PC interface:

- “Bluetooth connection PIN Code” is the PIN code used when making the initial connection to a PC (creating the Link Key). Default code is “12345678”

- “Reset Bluetooth Link Key” set a mark in the check box and click “OK” button. The new PIN Code is stored in the GateController™ and the current link key in the GateController™ is reset.

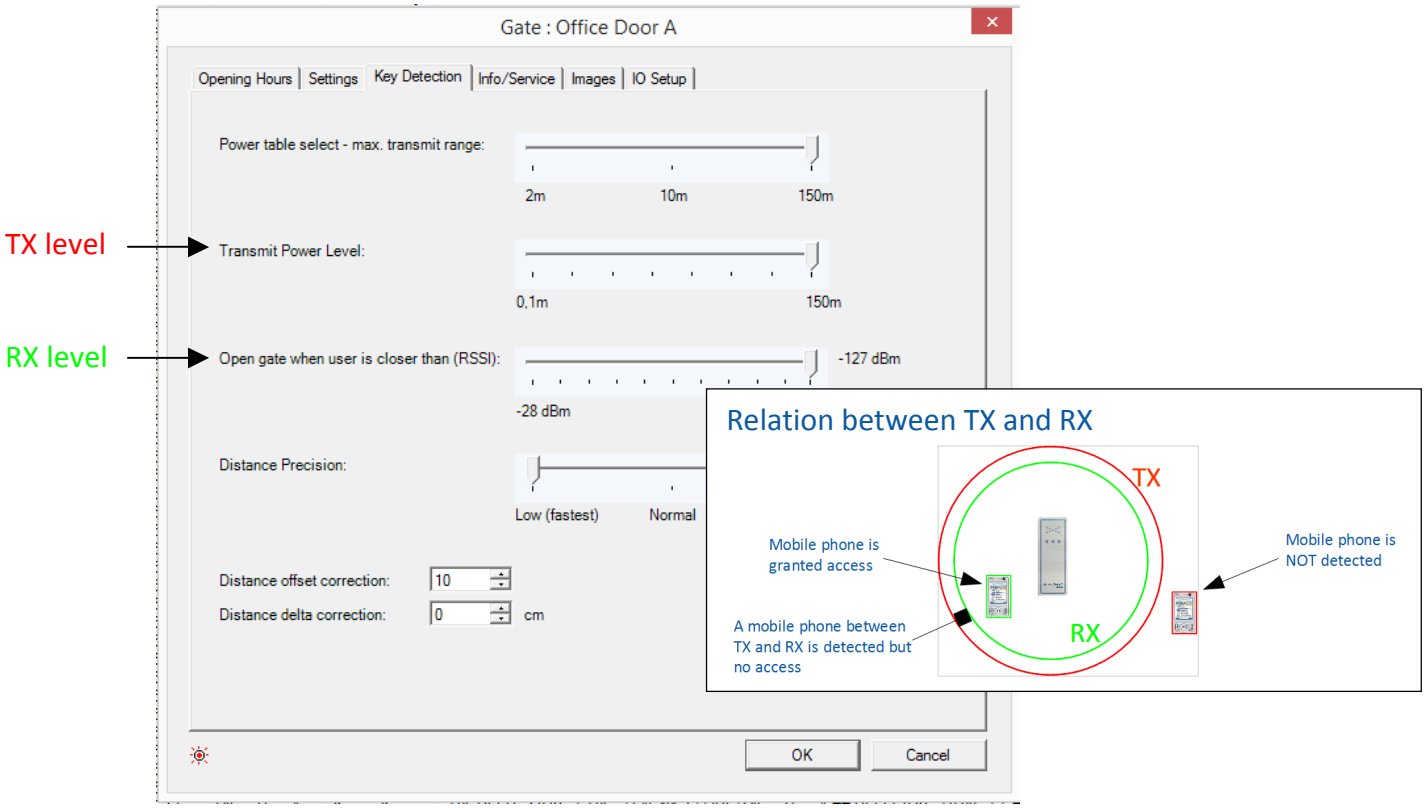
  Erase the link key on the PC before making a new connection with the new Bluetooth connection PIN code from the PC. The check box is automatically cleared when clicking the “OK” button.

  TIP!
  This is also useful if PcManagement™ must be moved to a new PC. Reset the Bluetooth Link Key and install PcManagement™ on the new PC. Create a new link key from the new PC.

  Refer to section 4.5.7.3 *Back-up of System Configuration and User Data*

4.11.3 Key Detection Range - Menu "Key Detection"

This menu allows you to adjust the user key (SBD key) detections parameters. What range (transmitting power) should be used with the GateController™, the distance measurement and the distance accuracy can be adjusted to the desired level for each door/barrier/gate:



- "Power table select - maz. transmit range" sets the transmitter power (TX) to the desired power table with a defined max. Click "OK". Reconnect GateController™ for the new power settings to take effect. Right click the GateController™ in the list and click "Restart Gate Controller". Default is 10m

- "Transmit Power Level" selects the used TX power level within the selected power table range. Default is 10m

- "Open gate when user is closer than (RSSI)" specifies the detection level (RX RSSI) for the users. I.e. how close must the user be to the GateController™ before access can be granted. There are 100 RSSI levels to choose from to make individual adjustments. Default is 37 dBm. The full RSSI range is -28 dBm to -127 dBm. A higher negativ RSSI level gives a longer range.

TIP!
Start with a large value and go down until detection is not possible anymore from the desired distance. Then go one step up again to find the correct values for the installation.

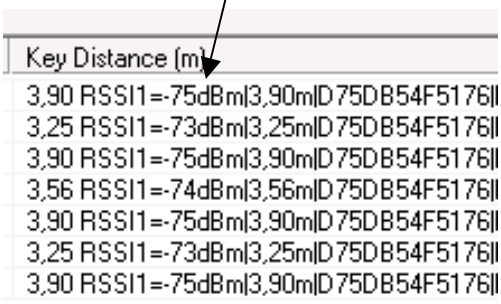
You can enable RSSI readout in the log to make adjustment easier by setting the

<config id="Show_RSSI" value="1" />

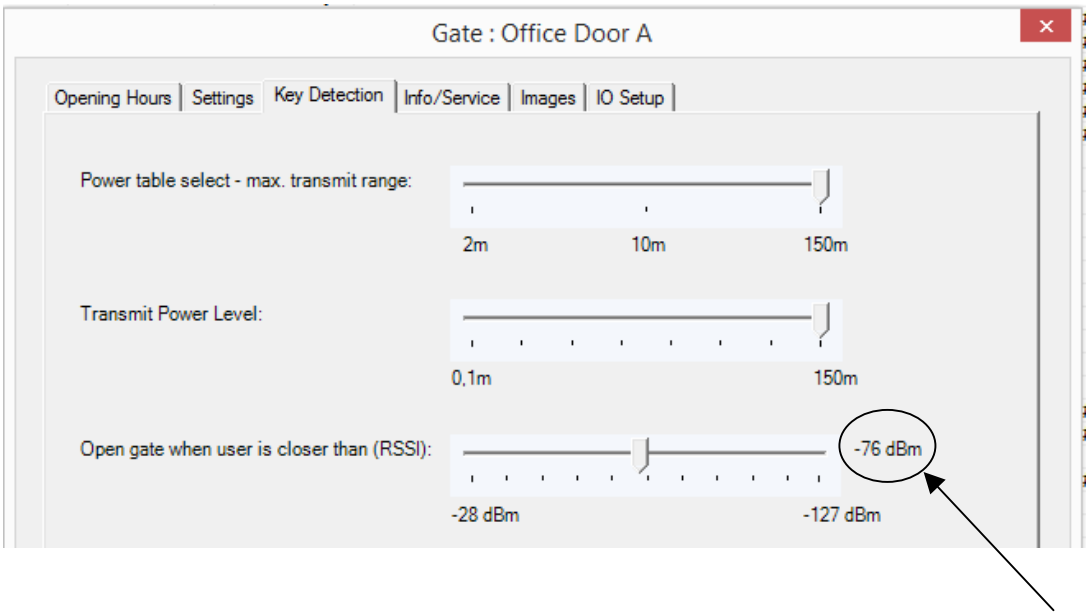
in the config.xml file. Default is disable <config id="Show_RSSI" value="0" />

Example of how to set the “Open gate when user is closer than (RSSI)” parameter:

Current RSSI level can be read under "Key Distance" in the log



E.g. Set RSSI to - 76 dBm to include device



In this example you should set the “Open gate when user is closer than (RSSI)” to minimum - 76 dBm to allow access for this device.

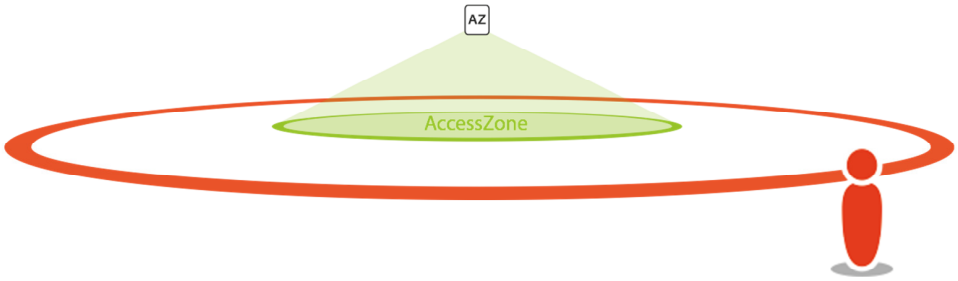
Caution!
The detection range can be influenced by the surroundings. If the detection range is not as expected the values can be adjusted up/down to find a suitable set of values. Please test and adjust as appropriate on location.

Note! The detection range may differ depending on the used device. Refer to 4.7.1 Add a new User – Menu “Settings” - > “Access” -> “Users”-> “Add” on how to compensate each user individually.

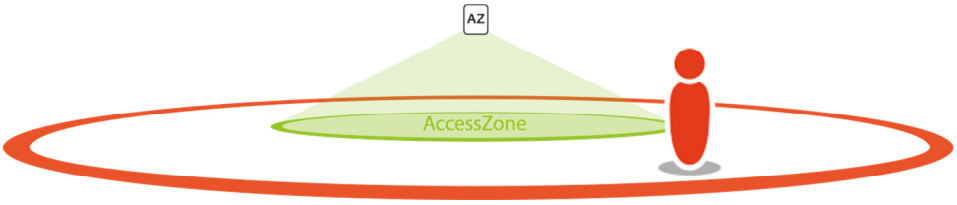
4.11.3.1 How to understand TX and RX parameters

The TX – and RX range should ideally lie on the same circle. It is recommended that the TX range is a little larger than the RX range.

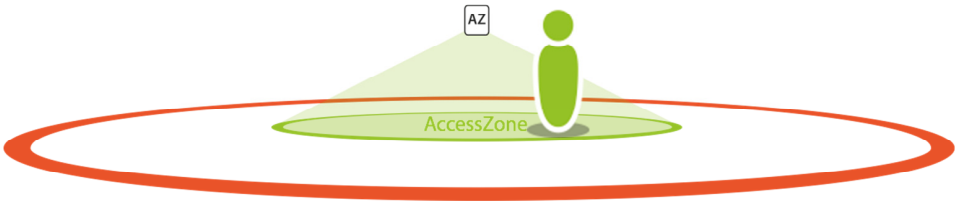
Scenario 1:
The user is outside the TX – and RX range and the user is not detected by the AccessZone® system. I.e. no access allowed



Scenario 2:
The user is now inside the TX circle and the AccessZone® system can read the unique ID from the mobile phone. However, access is not allowed because the user is outside the RX range.

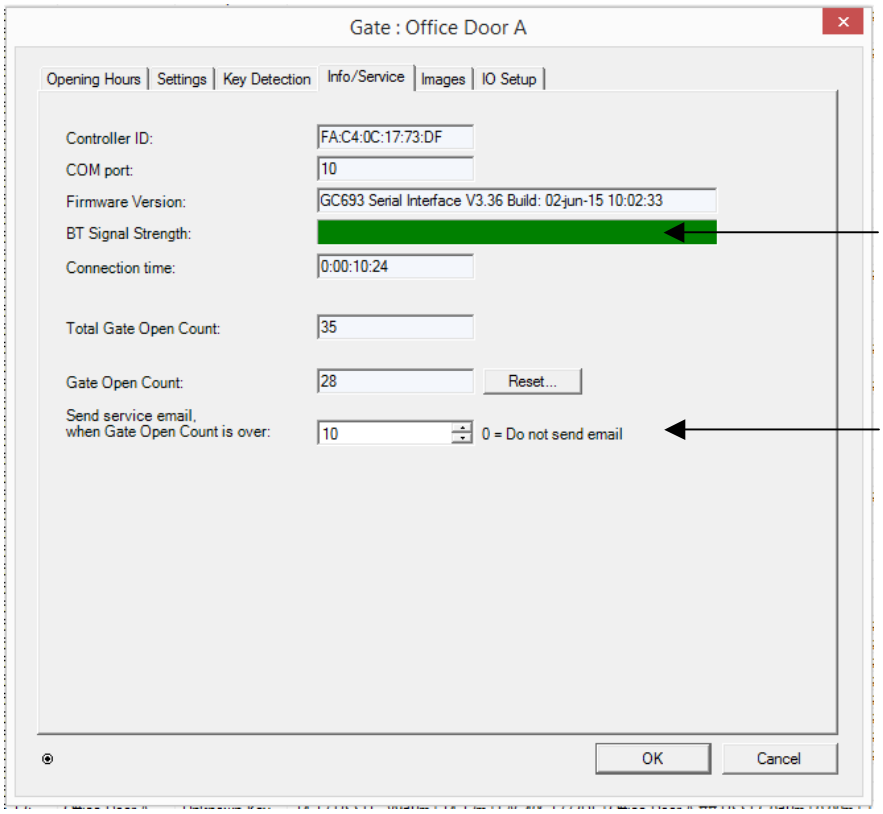


Scenario 3:
The user is now inside the TX circle and the AccessZone® system can read the unique ID from the mobile phone. The user is also within the RX range and access are allowed.



4.11.4 System Info - Menu "Info/Service"

The image shows specific information for the selected GateController™:



- "Controller ID" shows the connected GateController™ ID (the unique Bluetooth BD address)
- "COM port:" shows the COM port number for the connected GateController™
- "Firmware Version" shows the current firmware version in the GateController™
- "BT Signal Strength" shows a bar with the signal strength of the connection between the GateController™ and the PC. The signal strength is constantly monitored locally in the GateController™ and reported back.

  Note!
  This value is only of interest for GateControllers with a Bluetooth PC interface. If the signal strength is too weak it will automatically close the connection and try to reconnect to the GateController™
- "Connection time" shows how long time the PC and GateController™ has been connected

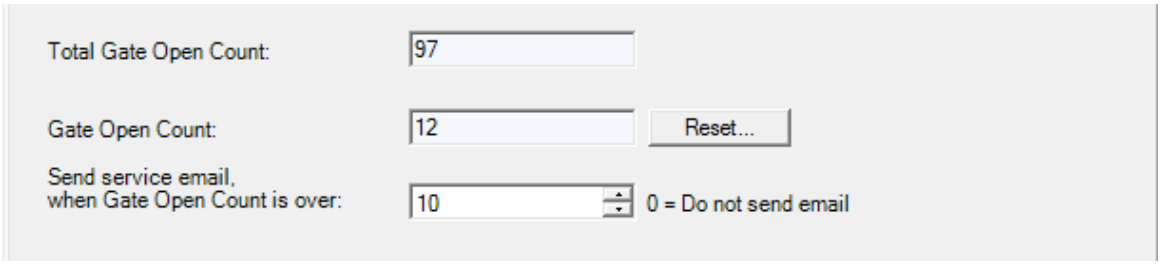
Service Email Indicator

This parameter can be used to schedule door/barrier/gate maintenance. An individual setting can be made for each door/barrier/gate.

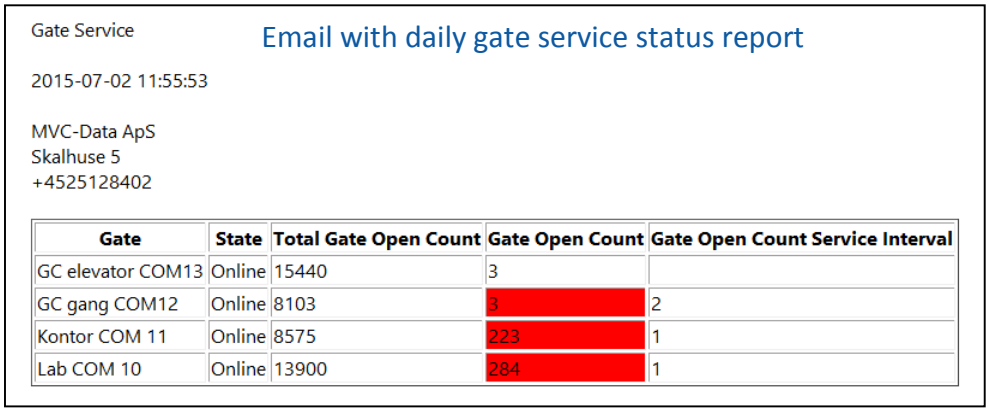
- "Total Gate Open Count"
  Shows the total number of granted accesses "openings" on the door/barrier/gate.

- "Gate Open Count"
  Shows the number of granted accesses "openings" since last service.

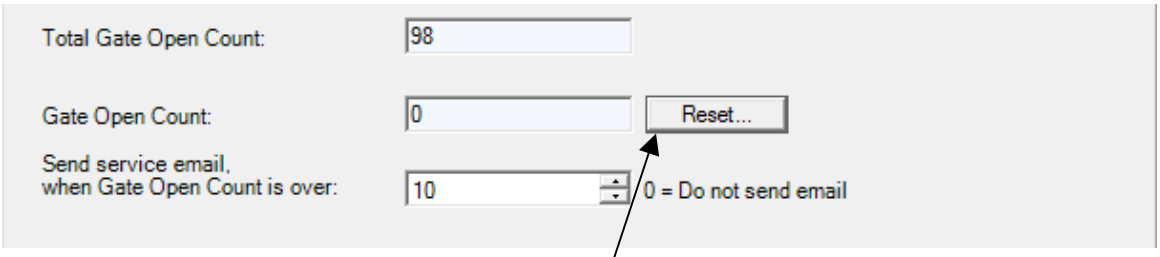
  When this counter is **above** "Send service emial, when Gate Open Count is over" a service email is schedule to be send on the specified time of day. Refer to section 4.10.4 *Notifications - Menu "Settings"-> "Program Settings" – "Notifications"*



Note!
An email will be sent daily with the status for all GateControllers in the system. E.g. is the GateController online. The "Gate Open Count" field is marked with red if value is higher than "Gate Open Count Service Interval".



Gate	State	Total Gate Open Count	Gate Open Count	Gate Open Count Service Interval
GC elevator COM13	Online	15440	3	
GC gang COM12	Online	8103	3	2
Kontor COM 11	Online	8575	223	1
Lab COM 10	Online	13900	284	1



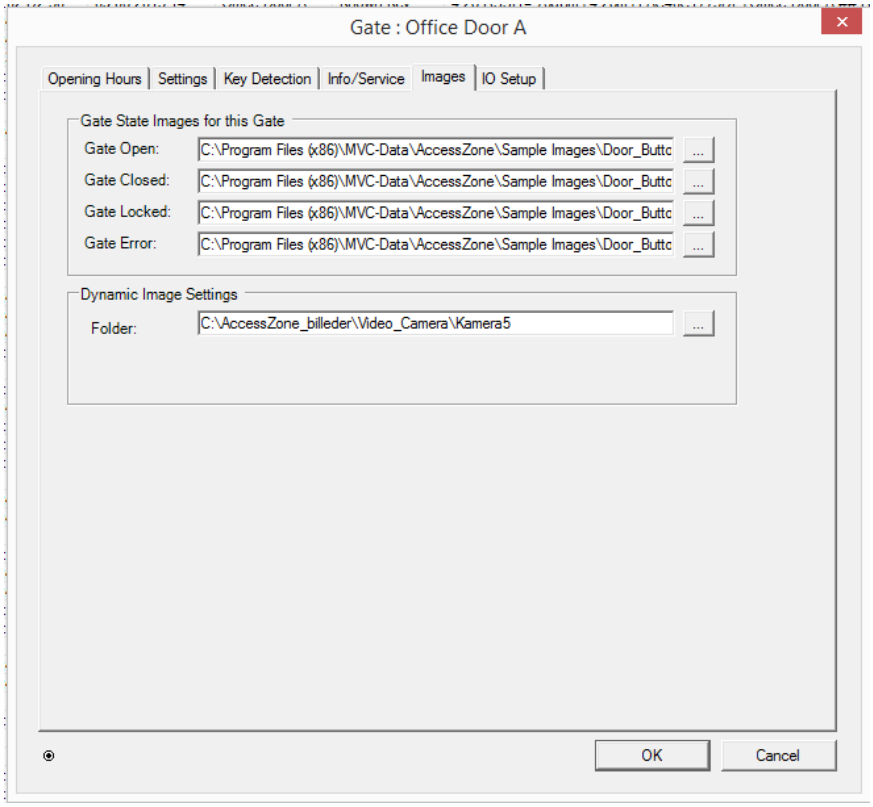
To clear service counter press the "Reset..." button.

- "Send service emial, when Gate Open Count is over"
  Set the trigger point when to receive the service notification for this gate.

  TIP!
  Set this parameter to 0 to disable service notification.

4.11.5 System Images - Menu "Images"

This image shows the used images for the specific GateController™:



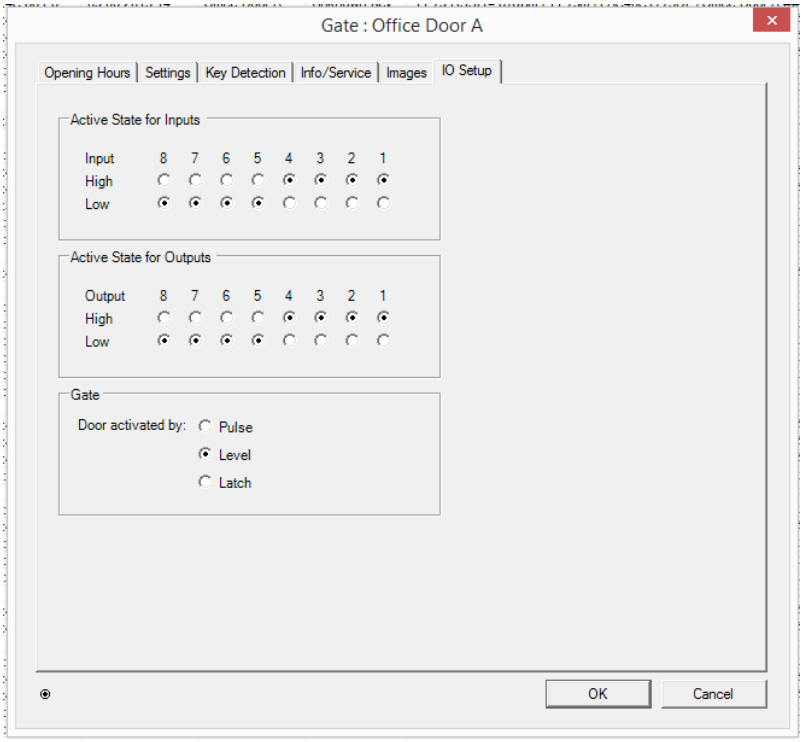
- "Gate State Images for this Gate" select the door/barrier/gate symbols to use with that particular GateController™. If nothing is specified the default images will be used. See section 4.10.2 *Images - Menu "Settings"-> "Program Settings" – "Area Views in Main Window"*

- "Dynamic Image Settings" specify the path to the images from the surveillance camera to be shown to the left of the CAD drawing of the secured area

TIP!
You can design your own symbols. Save the symbols in jpeg format and in the correct size matching the customized image (CAD drawing) of the secured area. You can also select some of the default delivered symbols (typically c:\Program Files\MVC-Data\AccessZone\Sample Images\..)

4.11.6 Input/Output Settings - Menu "IO Setup"

This view shows the Input/Output specific information for the selected GateController™:



- "Active State for Inputs" set the active levels (invert) for all inputs. The system can with this feature adapt to almost all sensors. Changes will take effect immediately.
  Default is input 1, 2, 3 and 4 set as high active.

- "Active State for Outputs" set the active levels (invert) for all outputs. The system can with this feature adapt to almost all kinds of door/barrier/gate logic. Changes will take effect on next event.
  Default is output 1, 2, 3 and 4 set as high active.

Default System Settings:

GC630/GC640/GC660/GC670/GC680/GC690:

Inputs: 1, 2, 3 and 4 are **high active** and 5, 6, 7, 8 are not used (don't care)
Output: 1 and 2 are **high active** and 3, 4, 5, 6, 7, 8 are not used (don't care)

GC3000 before firmware V2.78:

Inputs: 1, 2, 3 and 4 are **low active** and 5, 6, 7, 8 are not used (don't care)
Output: 1, 2, 3 and 4 are **high active** and 5, 6, 7 and 8 are low active

GC3000 from firmware V2.78:

Inputs: 1, 2, 3 and 4 are **high active** and 5, 6, 7, 8 are not used (don't care)
Output: 1, 2, 3 and 4 are **high active** and 5, 6, 7 and 8 are low active

All systems do not have all 8 inputs and outputs. Please refer to the appropriate Installation Manuel to see the number of I/Os for your system.

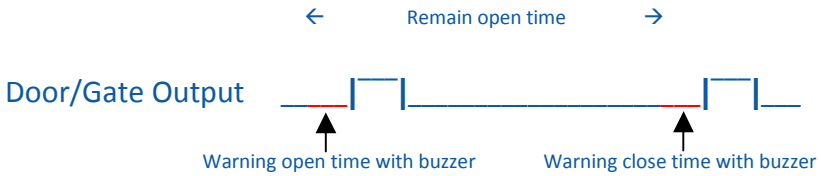
Caution!
Caution must be taken when changing the I/O parameters

- "Gate" specifies how the door/barrier/gate is activated:
  It supports 3 different door/gate output types to support different door/gate mechanisms.

  All types can be combined with a warning buzzer period before gate activation (warning buzzer can also be switched off)

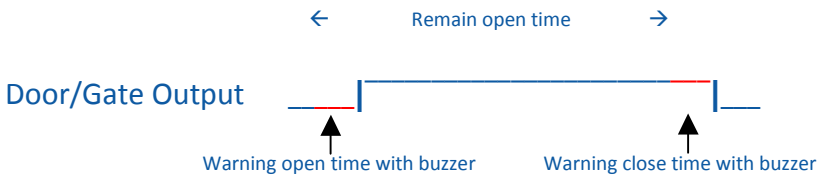
  - "Pulse"

  A 1 second pulse is used to activate the gate and another 1 second pulse is used to close the gate again after the timeout of the "Remain gate open time" period.



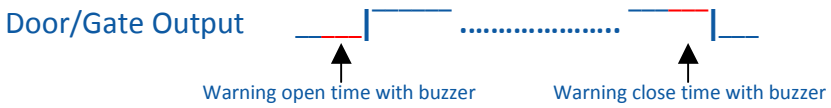
  - "Level"

  A pulse is used to activate the gate. The length of the pulse depends on the "Remain gate open time" period or if "Keep Open" feature is enabled and active.



  - "Latched" (toggle)

  The output is kept active (ON) from one valid access to the next where it changes back (toggle).



  Select the type suitable for your door, barrier or gate. Please refer to the door/barrier/gate manual for how to control it.

  TIP!

  - A barrier and a gate is usually a "Pulse" type. However, some barriers and gates have a built-in close timer. Use the "Level" type with a 1 s "Gate remain open time" to get a single open pulse.

  - A normal entry door with a door strike is usually a "Level" type.

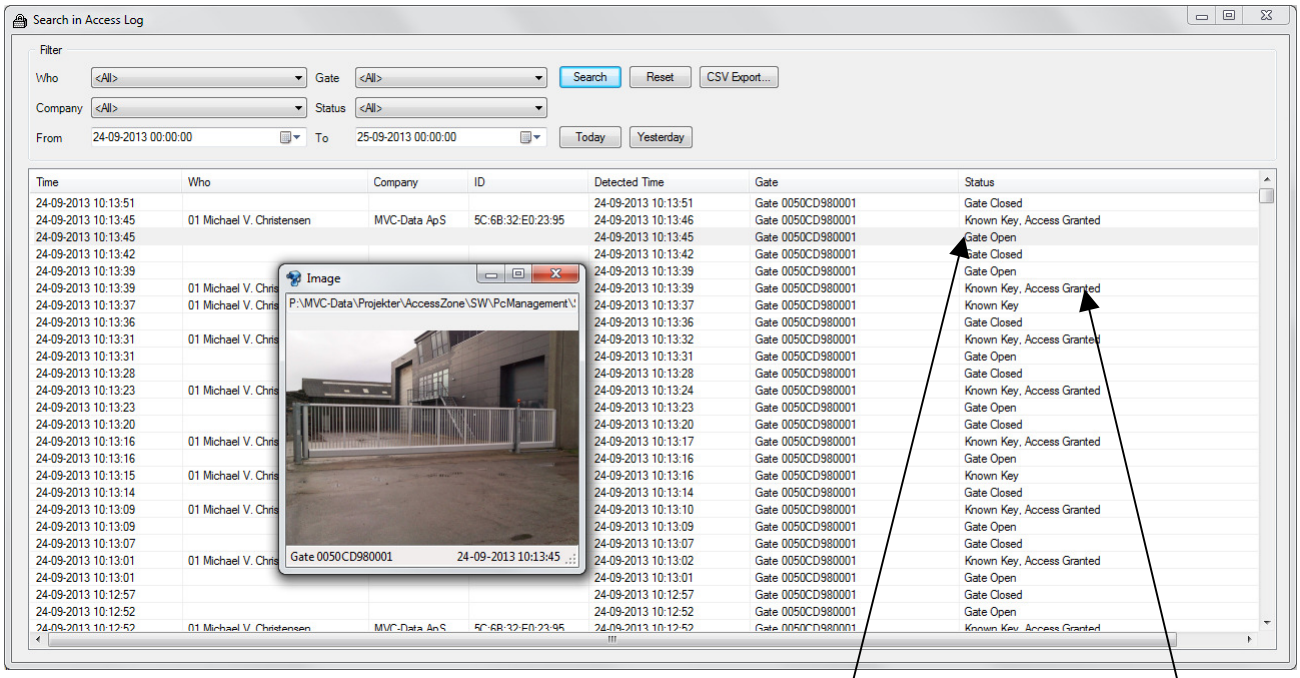
  - Latch (toggle) can be used with both doors/barriers/gates. It is recommended to use a user access PIN code with this type of signal. Special care must be taken when using the latched mode with the alarm arming procedure. Refer to 10.1.2 *Alarm Arming and Disarming*

  - The open signal can be inverted by changing the I/O settings. Refer to *Input/Output Settings - Menu "IO Setup"*

4.12 Database Search Tool – Menu “Search” -> “Access Log”

The tool is started from the main menu “Search” and “Access Log” or by pressing F3
This view shows how to make advanced searches in the event log database.

In example: Look for granted access for a particular user. All accesses on a particular door/barrier/gate or all accesses done from user from a specific Company (or other additional information added). Set the desired filters to narrow down the search results.



Click on the "Gate Open" to get the picture from the camera when the gate was opened.

Click on the "Known Key, Access Granted" to open the registered picture from the known user.

- “Who” select a specific user from the list
- “Gate” select a specific gate from the list
- “Company” select a specific company from the list
- “Status” select a specific event from the list
- “Today” get all the event from today
- “Yesterday” get all the event from yesterday

Click “Search” to start a search or click “Reset” to reset filters

TIP!
The “From” and “To” filters can be set to any date range or set down to a timer interval in seconds. Select the days from the calendar.

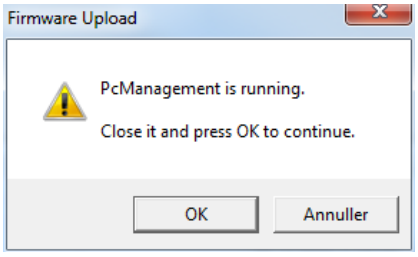
4.13 Tools – Menu "Tools"

The tools menu contains two tools "Firmware Upload" and "Replace Gate Controller".

4.13.1 Firmware Upload Tool - Menu "Tools"-> "Firmware Upload"

The "Firmware Upload" tool can be started from PcManagement™ or directly from the Windows installation menu "Programs". The tool can upload new firmware to the connected GateControllers. Refer to the "Firmware Upload User Manual".

Note!
PcManagement™ must be closed to release the used COM ports. The system will automatically start a dialog:



4.13.2 Replace GateController Tool - Menu "Tools"-> "Replace Gate Controller"

The "Replace Gate Controller" tool makes it easy to exchange a GateController™. I.e. all the settings and profiles are copied to the new GateController™ and the old GateController™ can be deleted.

- "Select Gate Controller to be replaced" select an existing GateController™ from the drop down list
- "Enter Controller ID for new Gate Controller" enter the ID of the new GateController™. The GateController™ ID must not existing in the system

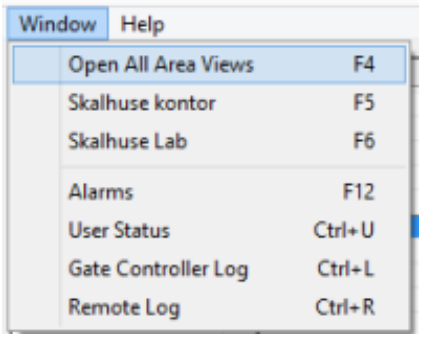
TIP!
The GateController™ ID can be found by connecting the system to PcManagement™.

Add the COM port number if not used before. Refer to section 4.10.1 *General Settings - Menu "Settings"-> "Program Settings" – "General"*. The system will automatically detect it as a new GateController™ and add it to the system. Refer to section 4.11.4 *System Info - Menu "Info/Service"* for how to read the ID.

Delete the GateController™ again to allow settings to be copied.

The new GateController™ can be connected to the system when the settings have been copied.

4.14 Tools – Menu “Window”



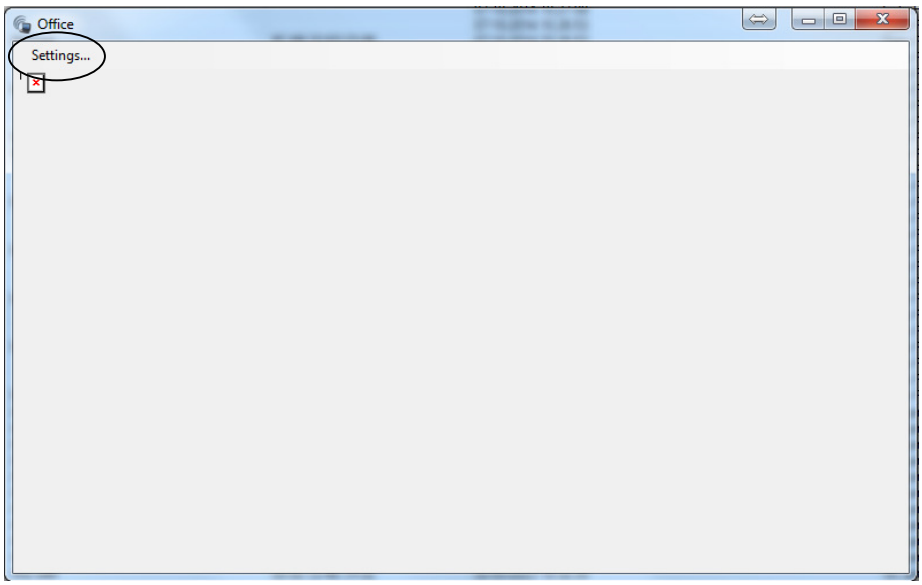
Under "Window" you can find and open up to 4 area views (if defined) and open 4 log files.

All are shown in individual windows and can be placed freely on the screen.

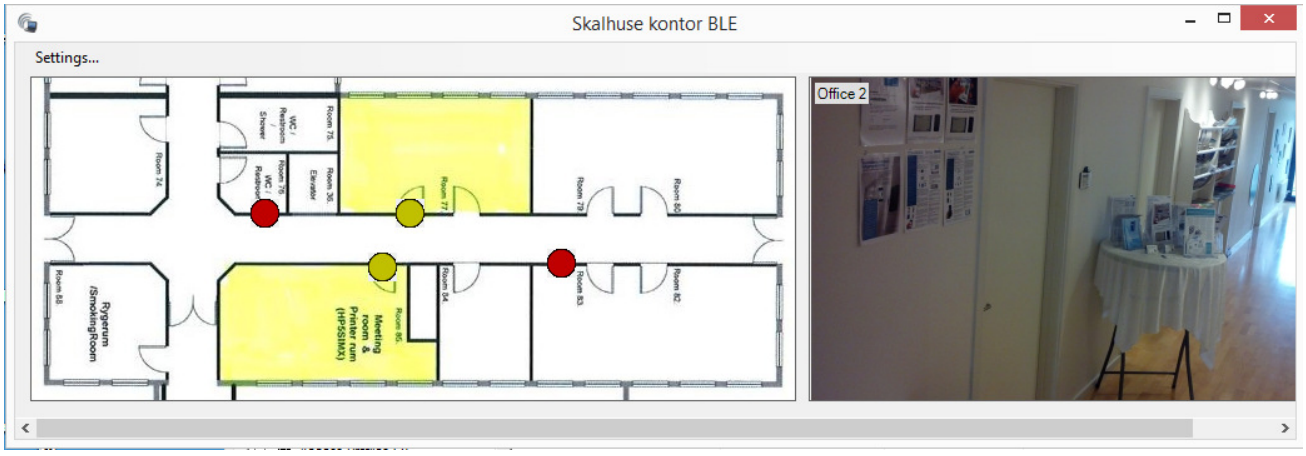
4.14.1 Area View

You can open all area views with the F4 key. A single area with F5 to F8 (if defined).

GateControllers can be added to the image and a video images can be shown to the left or under the area view. The area view is independently from the PcManagement main window and can be placed on a secondary screen to give a visual overview.



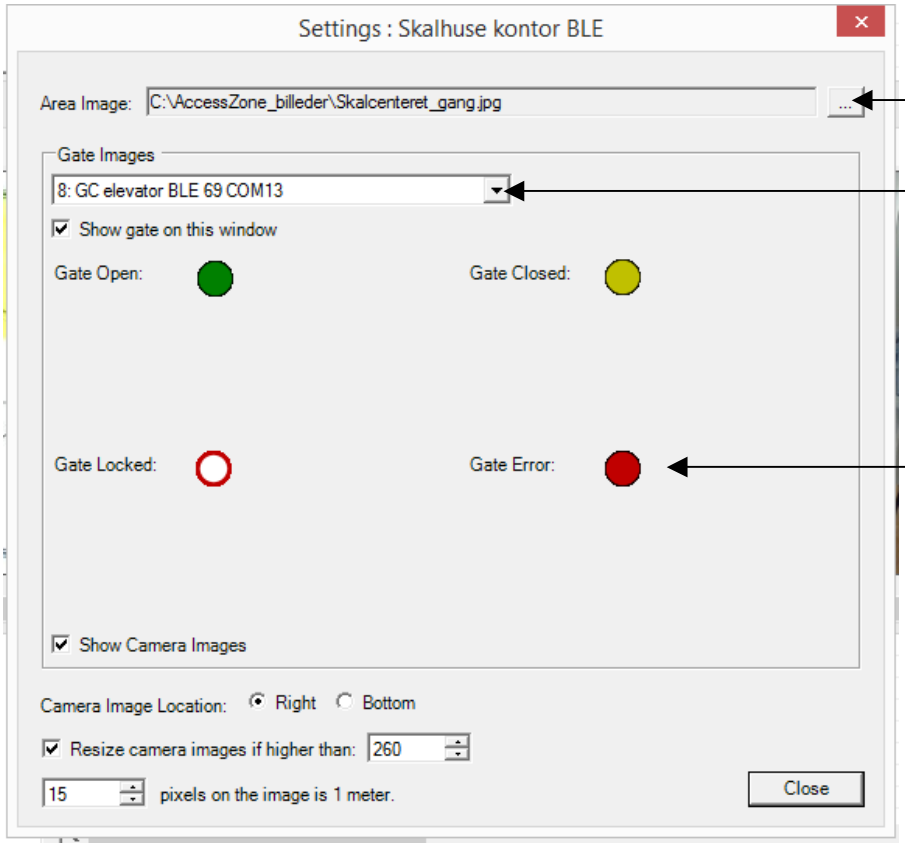
A new Area View has been defined but not setup yet.



An area view after setup up.

4.14.2 Area View Setup

The area view must be setup before use. Select the "Settings" in the upper left corner



Select file with the area image to use

Select the GateController and mark "Show gate on this window" to enable it on the area image

Double click a gate symbol to select a specific image to show on the area image. Default is shown here.

Click on the "Settings" to setup the area view:

- "Area Image" select a specific image file. I.e. a image or drawing of the secured area
- "Gate Images" select a specific gate from the list and mark "Show gate on this window" to enable it on the area view. Leave unmarked to skip GateController

  Run through the GateController list and add as required
- "Gate Open" the gate symbol showing an unlocked/open door or gate. Double click the symbol to select another image to show for this state

  Same for "Gate Closed", "Gate Locked" and "Gate Error" (not connected)
- "Show Camera Images" mark to enable show a video image
- Camera Image Location" select where the video image must be shown - to the right or under the area view
- "Resize camera images if higher than" to scale the video image so it fits the height of the area view
- "Pixels on image" is a to scale the image to the real world. Pixels for 1 meter

4.14.3 Log View

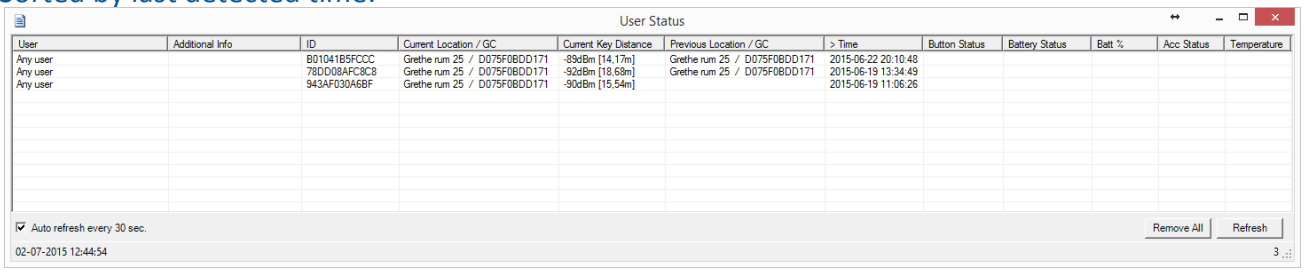
You can open 3 different logs to get an overview of the events.

- Alarms F12 Containing alarm messages
- User Status Ctrl+U Status information about the users
- Gate Controller Log Ctrl+L Communication status and user events
- Remote Log Ctrl+R Remote users login information

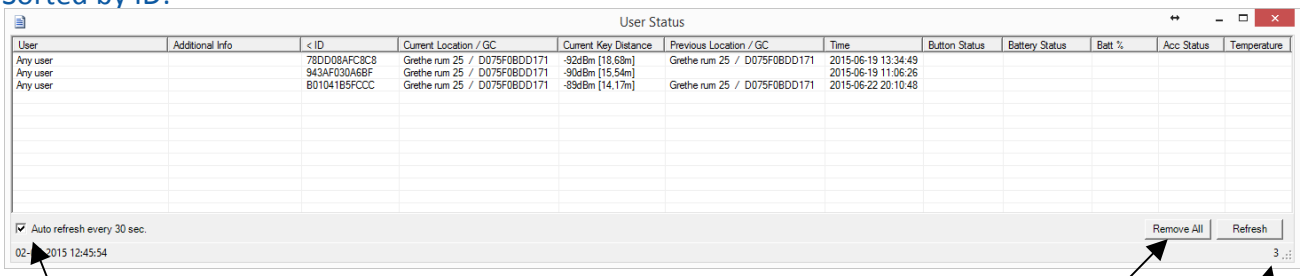
User Status example:

Multiple user status windows can be opened at the same with different sorting. Click on the column heading to change sorting:

Sorted by last detected time:



Sorted by ID:



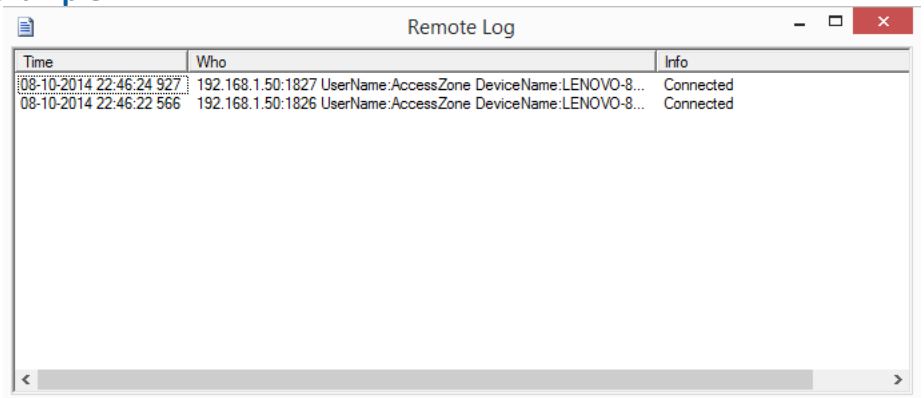
Mark "Auto refresh every 30 sec." to let the system automatically update the information.

Click "Remove All" to clear the list.

Click "Refresh" to manually refresh the information

Number of users in the list

Remote log example:



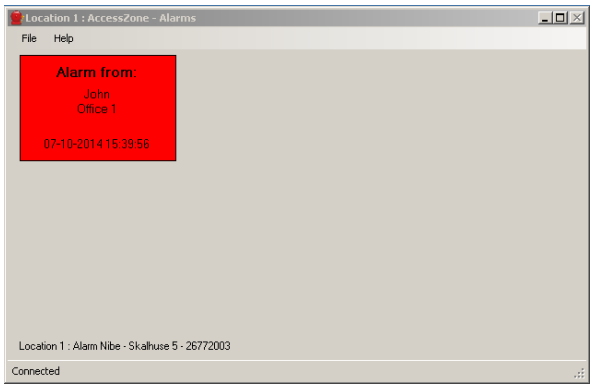
5 Clients

Different clients can be connected to the PcManagement server. This is usefull for distributing alarms to multiple PCs and remote access to do simple monitoring tasks.

Currently supported clients:

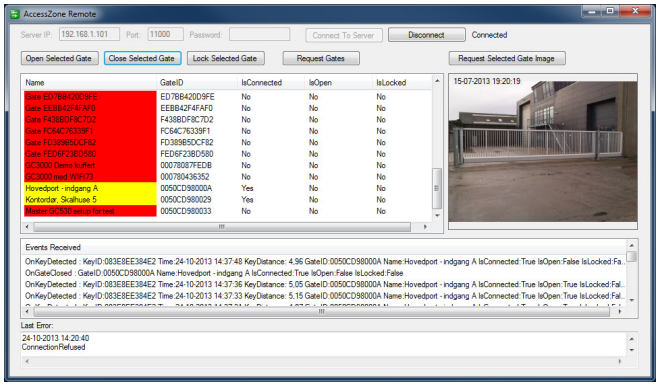
5.1 Alarm Client

Distribute alarm messages to other PC over the network:



5.2 Remote Client

Monitor whatever all gates are online. Open a gate remotely and watch video from the system



Refer to the User Manuals for the clients for more details.

6 Alarm Messages

The PcManagement Server can handle different alarms. The alarms are generated from the users using a GC110 Tag. The alarms are shown in PcManagement Server an on connected Alarm Clients.

The alarm messages can be customized in the PcManagement config.xml file.

Caution!

PcManagement server must be stopped before updating the messages.

In config.xml look for the "AlarmText" section.

Change the highligthed text in green:

```
<AlarmTexts id="0">
  <config id="IABIS_INCIDENT" value="Fall detected" />
  <config id="IABIS_INCIDENT_SAFE_SHORT" value="Alarm from" />
  <config id="IABIS_INCIDENT_SAFE_LONG" value=" Alarm from  (long)" />
  <config id="IABIS_INCIDENT_SAFE_STILL_PRESSED" value="Still Pressed" />
  <config id="IABIS_INCIDENT_OFF" value=" Alarm acknowledged " />
  <config id="IABIS_ACC_HIGH_G" value="High G detected" />
  <config id="IABIS_ACC_TILT" value="Motion detected" />
 </AlarmTexts>
```

Click save to update the <AlarmTexts id="0"> .... </AlarmTexts> section in your PcManagement system config.xml.

PcManagement server can be restarted after edit.

7 Mobile Phone as Access Key

Any Bluetooth enabled mobile phone can be used as access key. No software has to be installed on the mobile phone. Please refer to MVC-Data “How to Get the Bluetooth ID” paper (http://www.mvc-data.com/Misc.html).

MVC-Data ApS has developed some smart phones apps for iPhone and Android platform. Please refer to: http://www.mvc-data.com/Smart_Phones.html

The system will detect the mobile phone when it comes within the specified detection range.

TIP!
No pairing or search for devices must be active on the used mobile phone.

Steps:
1) Enable Bluetooth on mobile phone and set it to visible. Refer to the mobile phone's User Manual

2) Enter the 4 digit access PIN code when prompt (If PIN code is required) and click ”OK”

Note!
The time (Bluetooth inquiry scan time) a mobile phone uses to scan for other Bluetooth devices, that want to connect to it, is typically set to a low value to preserve battery power. I.e. the time to discover a nearby Bluetooth enabled mobile phone strongly depends on implementation details for a particular mobile phone.

8 GPS Antenna as Access Key

A Bluetooth GPS antenna is also suitable as a simple wireless key. It works fine with and without PIN code. The PIN is typically fixed to "0000" or "1234" so the PIN code can typically be left out. I.e. enable the GPS antenna without requiring PIN code.

The GPS antenna must typically not have an active connection to another Bluetooth device.

Note!
Most battery powered devices will automatically switch off after ex. 60 minutes to preserve battery power.

9 AccessZone® Bluetooth Tags

The AccessZone® Bluetooth Tags GC100 and GC230 are suitable as a simple wireless key. They work without PIN code. GC230 is also available with a fixed 4 digit PIN code.

They are available as battery powered hand-held devices (GC100) or as power wired devices for mounting on cars/trucks or wheelchairs (GC230).

Please refer to http://www.mvc-data.com/TAG.html for more information.

10 External Buttons

This section describes how the external buttons are used.

Please refer to the Installation Manual for how to connect external buttons as the REX push button and blocking operation sensors to the GateControllers.

10.1 Request Exit – REX Push Button

10.1.1 Request Exit

An external REX push button can be connected to the system. The REX push button must be installed on the secured side and will allow easy exit without using a mobile (except in the case of arming the alarm system).

The REX push button is also used with the Alarm Arming and Disarming feature.

The system will log all exits made with the REX push button.

10.1.2 Alarm Arming and Disarming

The system can arm and disarm an alarm system. The output is a level/latched output and the signal can be inverted.

The REX push button is also used with this feature.

10.1.3 Disarming the Alarm

The system will disarm the alarm by activating the output when a valid user has been detected.

The alarm is kept disarmed until armed again.

10.1.4 Arming the Alarm

The system will arm the alarm again when a valid user has been detected and the user presses the REX push button.

The alarm is kept armed until a valid user disarms it again.

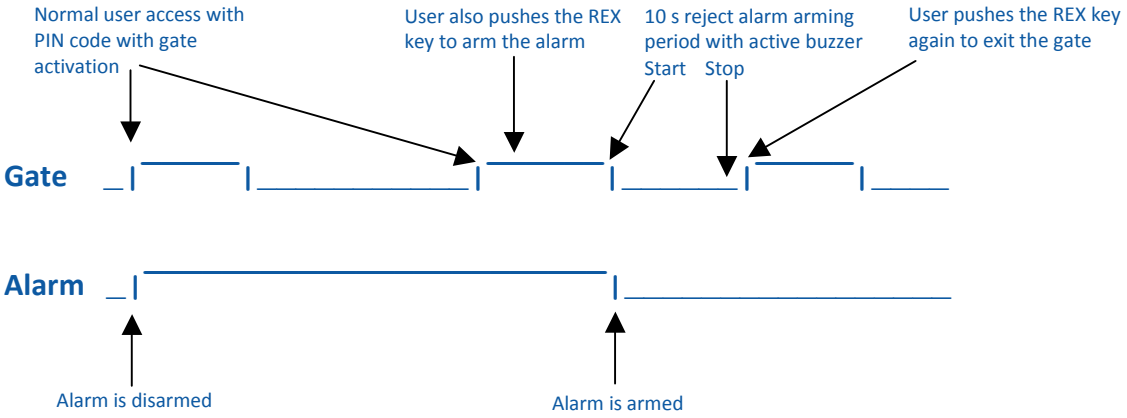
TIP!

Special care must be taken if the latched output is used for door activation. In this mode the door is already open (latched) when the alarm is going to be armed. The user must push the REX button before showing the user ID (mobile phone). This must be done within the remain open time period from the REX button was pressed be course the REX event is cleared after time-out of the remain open time period.

A suitable value for remain open time is 5-10 seconds for latched mode.

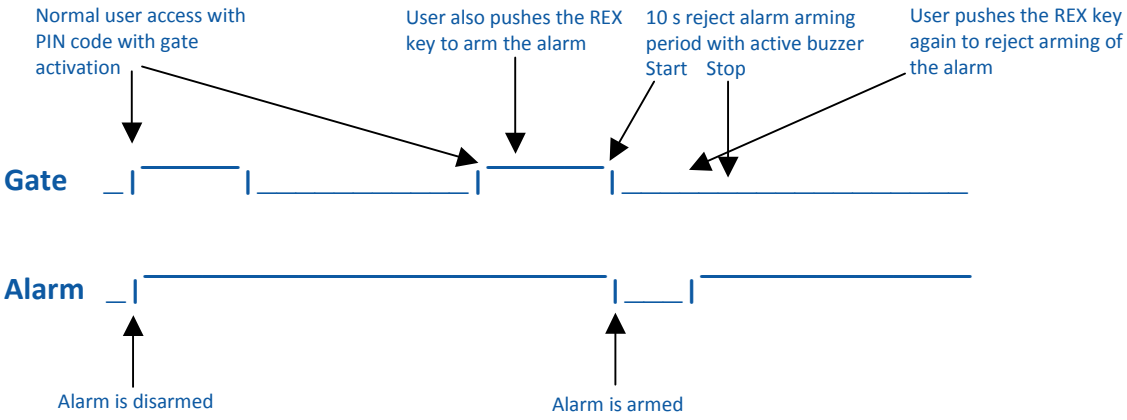
10.2 Timing Diagram of the outputs – Normal Access and Arming the Alarm

Case with active high outputs shown



10.3 Timing Diagram of the Outputs – Normal Access and Reject Arming of the Alarm

Case with active high outputs shown

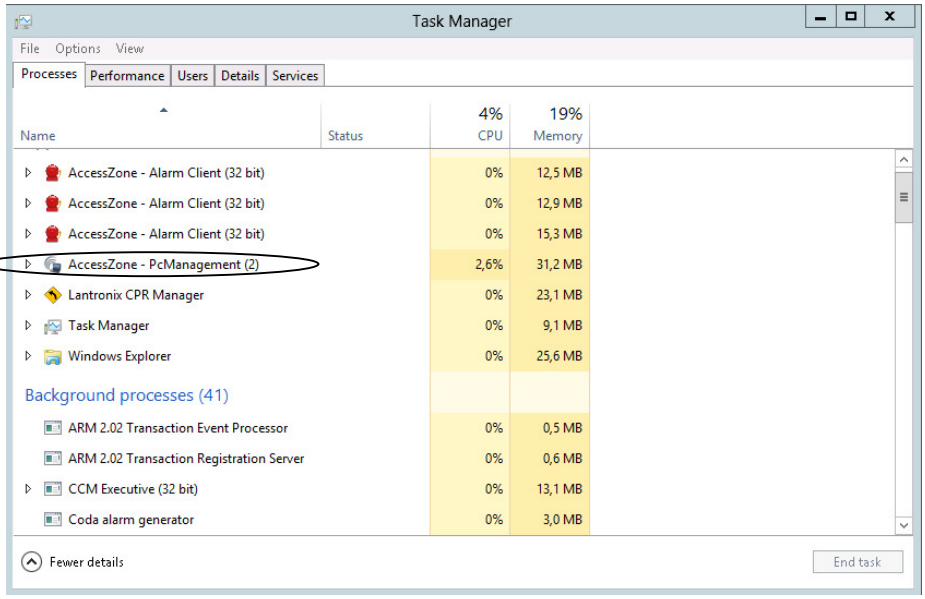


11 PcManagement running as Application or Background Service

PcManagement can be executed as an application or run as a service.

11.1 PcManagement running as a normal Application

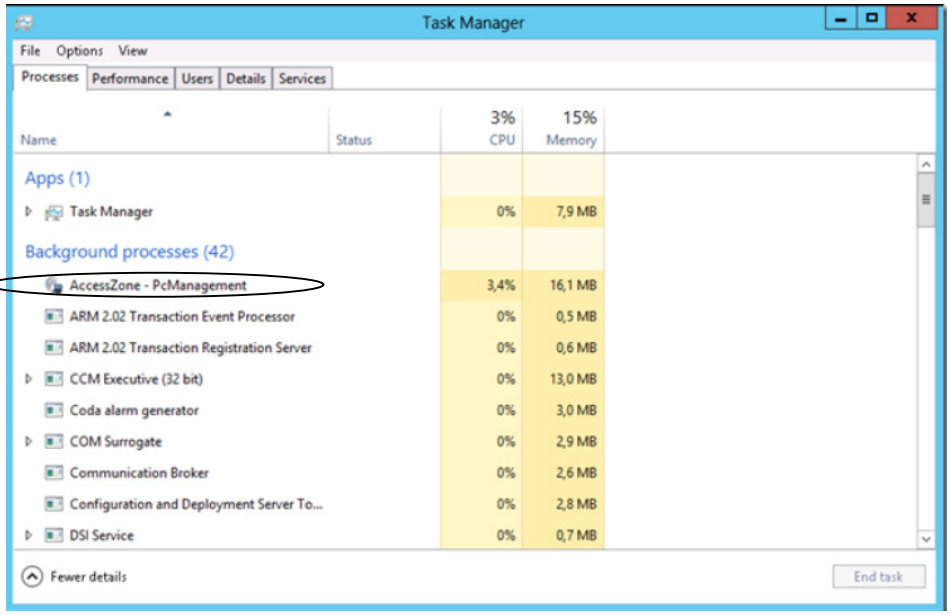
PcManagement is normally executed as an application with a full Graphical User Interface (GUI) to make changes to the system and give an overview of the running system. However, in some situation it is desireable to automatically start PcManagement (e.g. from Windows Task Scheduler) without having a user to log in first. I.e. it could be after a PC/server reboot.



11.2 PcManagement running as a background Service

When PcManagement is startet as a background service no GUI exists (running in Windows session 0). The system is fully operational but no changes can be made to the system and the current status cannot be monitored directly. However, the Remote Client™ can be used to see the status of all connected GateControllers™ (e.g. are they online or offline). Other clients like the Alarm Client™ can also still be connected to the server and is fully operational.

To start the GUI it is necessary to log in and stop the PcManagement server from the task managemer started with Ctrl+Alt+Delete and restart it as an application.



12 Default Factory System Settings

12.1 GC630/GC640/GC660/GC670/GC680/GC690 Series

The system configuration settings can be restored to factory settings:

Please follow the below steps:

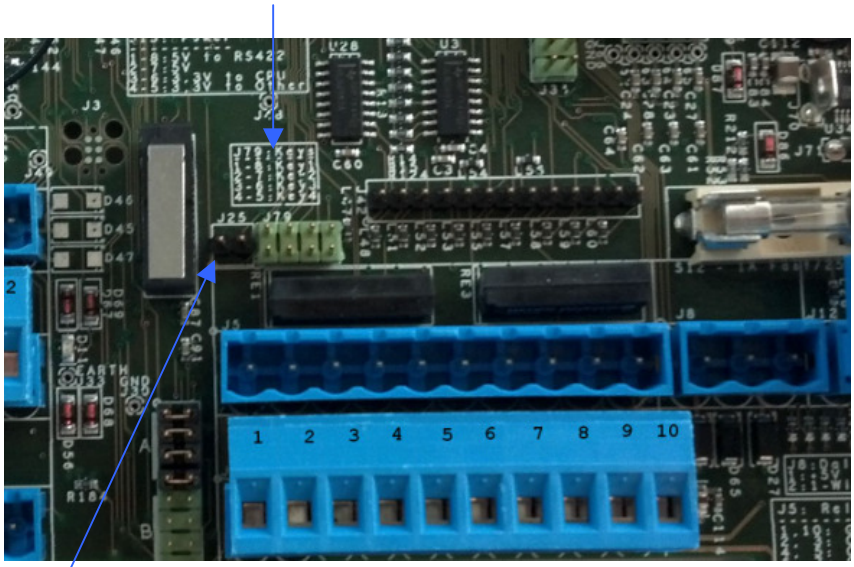
- Power off the device
- Short the 4 RS422 signals:
  - TxA to RxA
  - TxB to RxB
- Power on the device – Wait - a short beep acknowledges that the factory settings have been restored
- Power off the device again
- Reconnect the 4 RS422 signals
- Device can safely be re-powered with the restored factory settings.

Caution!
General caution must be taken when working with the wires to avoid short circuits etc.

12.2 GC3000 Series

Please follow the below steps:

- Power off the device
- Open the box
- Short the PIN 2-7 in J79 (it has no run-time functionality)
- Power on the device – Wait - a short beep acknowledges that the factory settings have been restored
- Power off the device again
- Remove the short the PIN 2-7 in J79 again
- Device can safely be re-powered with the restored factory settings



TIP!
Add a jumper on J25 to avoid tamper alarm - remember to remove the jumper again.